

# Neue kommerzielle Entwicklungen im Bereich von QKD

Ein Ausblick

von: Felix Trunk, Jasmin Neumann, Susanne Naegele-Jackson

## Inhalt

Abkürzungsverzeichnis .....	3
Einführung .....	4
1. Continuous-Variable QKD.....	5
Zustandsaustausch .....	5
Post-Processing .....	6
Aktuelle Situation, Vorteile und Probleme.....	8
Fazit .....	9
2. Twin-Field QKD .....	10
Protokoll .....	10
Realisierung .....	11
Vor- und Nachteile .....	13
Fazit .....	15
3. Multipoint QKD.....	16
Hardware-basierte Erweiterungen der P2P-Protokolle .....	16
Multiuser-Protokolle .....	19
Multiuser TF-Protokoll.....	19
Verschränkungs-basierte Protokolle .....	20
Weitere Multiuser Protokolle.....	21
Fazit .....	23
4. Koexistenz mit klassischem Datenverkehr .....	24
Störungen von QKD durch klassische Signale.....	24
Aktuelle Situation .....	25
Fazit .....	26
5. Photonic Integrated Circuits.....	27
Materialien .....	27
Eignung der verschiedenen QKD-Protokollfamilien für die Chipintegration .....	29
Hybride Systeme.....	30

Fazit .....	31
6. Multi-Core Fiber .....	32
Klassifizierung .....	32
Einsatz MCFs mit QKD .....	33
Fazit .....	34
7. High-Dimensional QKD .....	36
Kategorien .....	36
Zeit .....	37
Pfad .....	38
Orbitales Drehmoment .....	39
Frequenz .....	39
Hybride Verfahren .....	40
Fazit .....	41
Zusammenfassung .....	42
Tabellen- & Abbildungsverzeichnis .....	43
Literaturverzeichnis .....	44

## Abkürzungsverzeichnis

CDM	Carrier-Depletion-Modulation
CV	Continuous Variable
DEMUX	Demultiplexer
DoF	Degrees of Freedom
DPS	Differential Phase Shift
DSP	Digital Signal Processing
DV	Discrete Variable
DWDM	Dense Wavelength Division Multiplexing
EDFA	Erbium-Doped Fiber Amplifiers
FMF	Few-Mode Fiber
FPGA	Field Programmable Gate Array
FWM	Four Wave Mixing
HD	High Dimensional
LLO	Local Local Oscillator
LO	Local Oscillator
MCF	Multi-Core Fiber
MDI	Measurement-Device Independent
MEMS	Micro-Electro-Mechanical System
MZI	Mach-Zehnder Interferometer
OAM	Orbital Angular Momentum
OPLL	Optical Phase Locked Loop
P2MP	Point-to-Multipoint
P2P	Point-to-Point
PIC	Photonic Integrated Circuit
PLOB	Pirandola-Laurenza-Ottaviani-Banchi
PM	Prepare & Measure
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
SC-MCF	Strong-Coupling Multi-Core Fiber
SDM	Space Division Multiplexing
SDN	Software-Defined Networking
SKR	Secret Key Rate
SNR	Signal-to-Noise Ratio
SNS	Sending-Not-Sending
SNSPD	Superconducting Nanowire Single-Photon Detector
SPAD	Single Photon Avalanche Photodiode
SPD	Single Photon Detector
SPDC	Spontaneous Parametric Down-Conversion
SSMF	Standard-Single-Mode-Fiber
TDM	Time Division Multiplexing
TF	Twin-Field
THA	Trojan Horse Attack
TLO	Transmitted Local Oscillator
WC-MCF	Weak-Coupling Multi-Core Fiber
WDM	Wavelength Division Multiplexing

## Einführung

Die voranschreitende Entwicklung von Quantencomputern gefährdet die Sicherheit der aktuell verwendeten asymmetrischen kryptographischen Verfahren. Aus diesem Grund müssen zukünftig quantensichere Alternativen verwendet werden. Der Quantenschlüsselaustausch (engl. *Quantum Key Distribution* QKD) stellt einen vielversprechenden Ansatz dafür dar. Indem die grundlegenden Prinzipien der Quantenmechanik ausgenutzt werden, ist es möglich, gemeinsame Zufallszahlen zu erzeugen, die dann für die Verschlüsselung verwendet werden können.

Auch wenn es aktuell starke Limitierungen bezüglich Reichweite und Übertragungsraten gibt und normalerweise parallel zu der bestehenden Netzinfrastruktur neue Komponenten benötigt werden, um sogenannte Quantenkanäle zu schaffen, verspricht dieser Ansatz absolute Sicherheit, unabhängig von zukünftigen Entwicklungen in der Algorithmik und Technik.

Als Teil der zweiten Quantenrevolution befindet sich QKD am Übergang zwischen Forschung und Anwendung und erste kommerzielle Systeme sind bereits erhältlich. Aber die Entwicklung ist damit noch nicht abgeschlossen. Verbunden mit QKD existiert eine breit gestreute Forschungs- und Entwicklungsaktivität, um diese Technologie zu erweitern, unterstützen oder robuster zu gestalten. Dies hat zu vielen Entwicklungen und Innovationen in unterschiedlichen Richtungen geführt.

Ausgehend von der aktuellen Forschung hat sich dieses Dokument zum Ziel gesetzt, bedeutungsvolle Trends bereits jetzt genauer zu beleuchten, um abzuschätzen, was vermutlich in 5-10 Jahren technologisch von kommerziellen Geräten erwartet werden kann.

Der Fokus liegt daher auf neuen robusteren bzw. langreichweitigeren Protokollen (***Continuous-Variable QKD***, ***Twin-Field QKD***), auf der Entwicklung von der bisherigen *Point-to-Point QKD* zur ***Multipoint QKD*** für die vereinfachte Realisierung von Quantennetzwerken, sowie der **Koexistenz** mit klassischem Datenverkehr. Außerdem wird die **photonische Integration** von QKD und die Verwendung von ***Multi-Core Glasfasern***, vor allem für ***High-Dimensional QKD*** zur Erhöhung der Datenraten beleuchtet.

## 1. Continuous-Variable QKD

Während QKD initial ausgehend von diskreten Quantenzuständen, wie der Polarisation, in der Mitte der 1980er konzipiert wurde, ist seit der Jahrtausendwende bekannt, dass auch kontinuierliche Quanteneigenschaften zur Realisierung von QKD verwendet werden können. Diese als Continuous-Variable (CV) QKD bekannte Technologie unterscheidet sich fundamental von ihrem diskreten Counterpart.

Analog zu BB84 bei *Discrete-Variable* (DV) QKD, gibt es bei CV QKD das GG02 Protokoll [1], auf dem die meisten (kommerziellen) CV QKD Systeme basieren. Hier liegt daher auch der Fokus der beiden nachfolgenden Abschnitte, die grundlegende Konzepte und Begriffe erklären und hauptsächlich auf den Reviews [2], [3] basieren. So wird zunächst im Detail der Zustandsaustausch und das Post-Processing beschrieben, bevor die aktuelle Situation und Vor- & Nachteile diskutiert werden.

### Zustandsaustausch

Der mehrschrittige Gesamtprozess der CV QKD ist in *Abbildung 1* abgebildet und startet mit dem Zustandsaustausch.

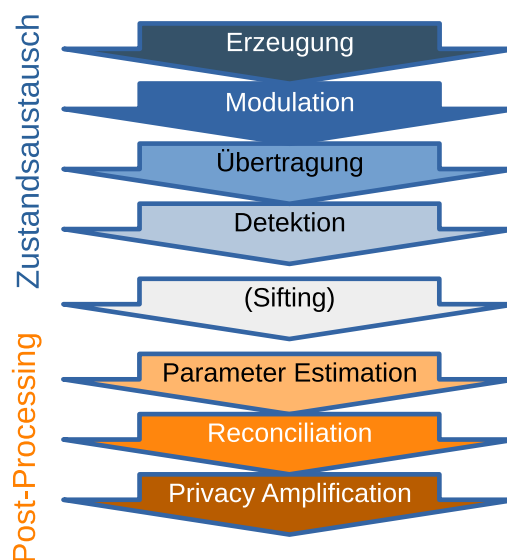


Abbildung 1: Prozessschritte der CV QKD.

**Erzeugung.** Bei CV QKD dienen nicht einzelne Photonen als Träger der Quanteninformation, sondern stattdessen werden spezielle Viel-Photonen-Zustände erzeugt. Bei GG02 und darauf basierenden Protokollen handelt es sich dabei um Zustände, die durch eine (kontinuierliche) komplexe Zahl beschrieben werden können, deren Real- und Imaginärteil auch als  $q/x$ - bzw.  $p$ -**Quadratur** bezeichnet wird. Üblicherweise werden sogenannte **kohärente Zustände** verwendet, bei denen die Varianz der beiden Quadraturen symmetrisch ist. Bei manchen, meist experimentelleren Realisierungen, werden allerdings auch sogenannte *Squeezed States* verwendet, bei denen die Quadraturen eine asymmetrische Varianz aufweisen.

**Modulation.** Bei der Präparation der Zustände für die QKD bestimmt Alice die Werte der Quadraturen durch Modulation von Amplitude und Phase von Laserpulsen, beispielsweise einer Gaußschen Verteilung folgend. Man spricht in diesem Fall dann von einer **Gaußschen Modulation**. Es gibt aber

auch experimentellere Protokolle, bei denen eine diskrete Modulation der Phase verwendet wird, wie beispielsweise in [4].

**Übertragung.** Die so generierten Zustände haben dann im Mittel bis zu 40 Photonen [5] und sind so zwar deutlich heller als die Zustände bei DV QKD, aber im Vergleich zu klassischen Signalen immer noch extrem schwach. Bei der Propagation zu Bob erfahren die Zustände analog zum DV QKD Fall Abschwächung und Störungen beispielsweise durch Lauschangriffe von Eve.

**Detektion.** Bei Bob werden die Quadraturen mittels kohärenter Detektion gemessen. Dabei unterscheidet man zwischen **homodyner Detektion**, die nur eine Quadratur messen kann, und **heterodyner Detektion**, bei der beide Quadraturen auf Kosten höheren Rauschens und erhöhter Realisierungskomplexität erhalten werden können. In beiden Fällen kommt es zu einer Interferenz zwischen dem Quantensignal und einem *Local Oscillator* (LO) Signal, das effektiv dem Laserpuls ohne Alices Modulation entspricht, und der anschließenden Messung von Lichtintensitäten. Bei der homodynen Detektion bestimmt die Phase zwischen den beiden Signalen, welche Quadratur gemessen wird und es wird zufällig entschieden, welche Quadratur gemessen werden soll. Bei der heterodynen Detektion kann es sich entweder effektiv um zwei parallele homodyne Detektionen handeln oder es wird mittels *Downsampling* des Quantensignals durch einen LO mit einer leicht verschobenen Frequenz realisiert, was ermöglicht aus den gemessenen Lichtintensitäten per *Digital Signal Processing* (DSP) beide Quadraturen zu erhalten.

Es gibt zwei verschiedene Ansätze, wie das LO Signal Bobs Detektor zur Verfügung gestellt werden kann. Zum einen ist es möglich, dass das LO Signal direkt von Alice mitgeschickt wird. Dies wird häufig als *Transmitted LO (TLO)* bezeichnet. Allerdings weist dieser naheliegendste Weg einige Probleme auf. Zum einen ist das LO Signal mehrere Größenordnungen stärker als das Quantensignal und kann somit zu starken Störungen führen. Zum anderen limitiert dieses Verfahren die maximal erreichbare Distanz, da es aufgrund der Dämpfung bei großen Distanzen dazu kommen kann, dass das LO Signal zu schwach für die kohärente Detektion ist. Außerdem ergeben sich zusätzliche Seitenkanalangriffe durch dieses Schema. Deswegen setzt sich seit einiger Zeit ein anderes, als *Local LO (LLO)* bezeichnetes Verfahren zunehmend durch. Dabei wird das LO Signal am Detektor erzeugt und die notwendigen Frequenz- und Phaseninformationen mittels speziellen Referenzpulsen zur Verfügung gestellt, die als **Pilot Signale** bezeichnet werden. Auch wenn dieses Verfahren theoretisch höhere Reichweiten ermöglichen kann und sicherer ist, ist es auch deutlich komplexer und weist aktuell üblicherweise eine geringere Performanz auf, insbesondere bei hohen Wiederholungsraten und Distanzen. Daran sind vor allem Probleme beim verlässlichen Synchronisieren der Phase und das daraus resultierende Phasenrauschen schuld [6]. Sowohl bei TLO als auch LLO wird Zeit-, Polarisations- und/oder Wellenlängenmultiplexing verwendet um LO bzw. Pilot Signal von dem Quantensignal zu trennen. Außerdem werden üblicherweise automatisierte Feedbacksysteme verwendet, um Phasen- und Polarisationsstörungen auszugleichen und eine gute Zeitsynchronisation zu erreichen.

**Sifting.** Bei der Verwendung von homodyner Detektion erfolgt in einem nächsten Schritt eine Verständigung darüber, welche Quadratur von Bob gemessen wurde, ein Prozess der auch als *Sifting* bezeichnet wird. Danach liegen bei Alice und Bob korrelierte kontinuierliche Größen vor, aus denen im Post-Processing die kryptographischen Schlüssel erhalten werden.

## Post-Processing

Bei CV QKD ist im Gegensatz zu DV QKD das Post-Processing sehr komplex und rechenintensiv, sodass es nicht unüblich ist, dass leistungsstarke Grafikkarten benötigt werden und hier das Bottleneck bezüglich Wiederholungsrate oder Reichweite liegt:

**Parameter Estimation.** In einem ersten Schritt, der sogenannten **Parameter Estimation**, werden Kanal-, Detektor- und Signalparameter (wie z.B. die *Signal-to-Noise Ratio* (SNR), *Excess Noise*, etc.) bestimmt und die Kovarianzmatrix der Korrelation berechnet, um damit abzuschätzen, ob bzw. wie viele kryptographische Schlüssel aus den Korrelationen in den ausgetauschten Zuständen erhalten werden können. Im Gegensatz zu DV QKD wird hier also nicht erst direkt aus den einzelnen Quantensignalen ein korrelierter Bitstream erhalten und dann über die *Quantum Bit Error Rate* (QBER) bestimmt, wie viele geheime Schlüssel möglich sind. Die Parameter Estimation ist daher sehr wichtig, da sie die Vertraulichkeit der später erzeugten Schlüssel sicherstellt, aber insbesondere bei großen Distanzen ist die Abschätzung der Parameter mit hinreichender Genauigkeit oft sehr ineffizient und/oder rechenaufwendig.

**Reconciliation.** Falls eine Schlüsselerzeugung möglich ist, folgt dann die sogenannte **Reconciliation**, in der sich ausgehend von den gemeinsamen Korrelationen in den kontinuierlichen Größen auf einen fehlerkorrigierten Bitstream geeinigt wird. In diesem Schritt findet also die Diskretisierung der kontinuierlichen Variablen und Fehlerkorrektur statt. Die Effizienz liegt hierbei oft bei >90% ([6] - [11]), allerdings kann die Reconciliation auch fehlschlagen, was durch die *Frame Error Rate* (FER) beschrieben wird. In den ersten Realisierungen wurde versucht, dass Bob sich durch *Direct Reconciliation* ausgehend von seinen detektierten Daten an die Modulation von Alice angleicht. Da im Allgemeinen aber Eve stärker mit Alice korreliert ist als mit Bob, wird bei diesem Ansatz grundsätzlich eine  $SNR > 1$  benötigt um QKD Schlüssel erzeugen zu können, was in der Literatur auch als 3 dB Problem bekannt ist und die möglichen Distanzen stark limitierte. Inzwischen wird stattdessen **Reverse Reconciliation** angewandt, bei der Alice versucht zu rekonstruieren was Bob gemessen hat. Abhängig von der vorliegenden SNR werden verschiedene Reconciliation Verfahren verwendet. Während bei hoher SNR oft *Slice Reconciliation* [12] verwendet werden kann, bei der die kontinuierlichen Variablen zuerst diskretisiert und dann fehlerkorrigiert werden, hat sich bei geringer SNR ein als *Multidimensional Reconciliation* [13] bezeichnetes Verfahren durchgesetzt, bei dem mehrere kontinuierliche Variablen gleichzeitig in einem 8D Raum betrachtet werden, wodurch selbst bei  $SNR \sim 0.002$  noch Reconciliation realisiert wurde [7]. Häufig werden dabei sogenannte *Multiedge-Type Low-Density Parity-Check* (MET LDPC) Codes [12] zur Fehlerkorrektur angewandt. Da das ausgewählte Reconciliation Verfahren immer nur in einem gewissen SNR Bereich effizient arbeitet<sup>1</sup>, wird z.T. sogar durch künstliches Rauschen die SNR absichtlich reduziert, wie beispielsweise in [5].

**Privacy Amplification.** Abschließend erfolgt, analog zu DV QKD, klassische **Privacy Amplification**, wobei aus dem bei Alice und Bob vorliegenden Bitstream ein kürzerer Bitstream mit den kryptographischen Schlüsseln erzeugt wird. Für diesen kann dann garantiert werden, dass keine Informationen bei der potentiellen Lauscherin Eve vorliegen. Aktuell werden häufig Verfahren basierend auf *Toeplitz* Matrizen angewandt [14]. Dabei wird der Bitstream aus der Reconciliation mehrfach mit nicht-quadratischen, zufälligen Matrizen multipliziert. Für Toeplitz-Matrizen können die notwendigen Multiplikationen und der Austausch der Matrizen sehr effizient realisiert werden, während die Berechnung der inversen Matrizen restriktiv komplex ist. Durch jeden Multiplikationsschritt wird somit vorhandenes Wissen von Eve über bestimmte Bits reduziert. Die notwendige Verkürzung des Bitstreams basiert auf einer Abschätzung der sicheren Schlüsselrate ausgehend von den Ergebnissen der Parameter Estimation. In diesem Kontext sind die sogenannten **Finite-Size Effekte** sehr wichtig [15]. Da nur eine endliche Anzahl an ausgetauschten Zuständen vorliegt, kommt es bei der Bestimmung der Parameter immer zu statistischen Unsicherheiten die

---

<sup>1</sup> Beispielsweise wird in [7] für SNRs zwischen 0.46 und 0.03 ein Multidimensional Reconciliation Verfahren basierend auf MET LDPC angewandt. Bei niedrigerer SNR (bis  $\sim 0.002$ ) muss dort auf ein anderes Multidimensional Reconciliation Verfahren zurückgegriffen werden, während bei höheren SNRs Slice Reconciliation verwendet wird.

pessimistisch abgeschätzt werden müssen. Daher ist die sogenannte asymptotische *Secret Key Rate* (SKR), die diese Effekte nicht berücksichtigt, immer größer als die praktisch sicher nutzbare SKR mit Finite-Size Effekten. Da bei CV QKD durch die Verwendung von kontinuierlichen Variablen diese Effekte stärker ausgeprägt sind als bei DV QKD, ist es notwendig, Blöcke mit vielen einzelnen Messpunkten ( $>10^5$ , in [7] auch bis zu  $10^{12}$  bei hohen Reichweiten) gleichzeitig zu betrachten.

Aufgrund der großen Wichtigkeit des Post-Processings, sind neben Verbesserung der CV QKD Hardware auch die Entwicklung neuer Verfahren zur Parameter Estimation und Reconciliation Gegenstand der aktuellen Forschung, um höhere Reichweiten und SKRs zu ermöglichen. Einige CV QKD Experimente versuchen außerdem durch Vertauschung der beiden ersten Post-Processing Schritte die globale Effizienz zu erhöhen, indem nur Messpunkte, bei denen die Reconciliation fehlgeschlagen ist, zur Parameter Estimation verwendet werden [7], [10].

### Aktuelle Situation, Vorteile und Probleme

Tabelle 1 gibt einen Überblick über aktuelle CV QKD Experimente bzw. Testbeds. Der Fokus liegt hier auf Realisierungen von Protokollen mit kohärenten Zuständen und Gaußscher Modulation unter Berücksichtigung von Finite-Size Effekten, da diese die weiteste Verbreitung aufweisen. Falls bei Experimenten das Post-Processing nicht in Echtzeit erfolgt, sondern stattdessen initial die Daten nur abgespeichert und erst später weiterbearbeitet werden, so ist dies entsprechend angemerkt. Aktuelle Realisierungen von Protokollen z.B. mit Squeezed States oder Diskreter Modulation werden u.a. in [2] präsentiert.

Quelle	Jahr	TLO/ LLO	homodyne/ heterodyne Detektion	SKR	Reichweite (Dämpfung)	Wiederholungsrate
<b>Anmerkungen</b>						
[10]	2019	TLO	homodyn	6 kbps	50 km (11.6 dB)	5 MHz
Feldexperiment mit kommerziellen Fasern						
[7]	2020	TLO	homodyn	127k/12k/6 bps	27/99/203 km (4.4/16/32.5 dB)	5 MHz
Aktueller CV QKD Reichweitenrekord via top-end Laser, Faser, Detektor und Reconciliation Schema; Post-Processing mit $10^{11}$ - $10^{12}$ Blockgröße						
[5], [16]	2023	LLO	heterodyn	10k/10 bps	10/20 dB	10 MHz
Feldexperiment von Huawei im MadQCI Testbed mit ungepaarten Sendern und Empfängern bei variabler Wellenlänge, künstliches Rauschen für effiziente Reconciliation, umfangreiches DSP; vermutlich keine Berücksichtigung von Finite-Size Effekten!						
[6]	2023	LLO	heterodyn	25.4 kbps	100 km (15.4 dB)	10 MHz
Nicht-Echtzeit Post-Processing mit $10^9$ Blockgröße, umfangreiches DSP						
[8]	2024	LLO	homodyn	0.24 Mbps	28.6 km (7.5 dB)	0.5 GHz
Photonisch integrierter QKD Empfänger mit externen Lasern, Nicht-Echtzeit Post-Processing mit $10^9$ Blockgröße, umfangreiches DSP						

Tabelle 1: Übersicht zu aktuellen CV QKD Experimenten und Testbeds

CV QKD bietet einige Vorteile gegenüber der etablierten DV QKD. So liegen beispielsweise die theoretischen Obergrenzen von Reichweite und SKR bei CV QKD höher als die des weitverbreiteten BB84 Protokolls. Außerdem ist die Realisierung von CV QKD Systemen, insbesondere die Erzeugung und Detektion der Quantenzustände, deutlich einfacher möglich und mit Standard Telekommunikationsequipment umsetzbar. So werden keine *Single-Photon Detectors* (SPDs) benötigt



und es können effiziente kommerzielle Detektoren bei Raumtemperatur eingesetzt und hohe Wiederholungsraten erreichen werden. Auch bei der Zustandspräparation können direkt konventionelle Laser verwendet werden, anstelle von teuren Einzelphotonenquellen oder komplexen Verfahren mit *Decoy-States*, wie sie bei DV QKD nötig sind. Zusätzlich ist es möglich, sowohl bei der Erzeugung als auch bei der Detektion, DSP z.B. zum *Pulsshaping*, für SNR Optimierungen oder für Phasenkorrekturen einzusetzen, wodurch die Komplexität der Systeme reduziert werden kann [3], [16]. Abschließend soll hier noch erwähnt werden, dass CV QKD sich gut für die photonische Integration eignet, was höhere Wiederholungsraten im GHz Bereich und billigere Systeme verspricht. Außerdem ermöglichen die höhere Signalintensität und frequenzselektive Detektion eine leichtere Koexistenz mit klassischem Datenverkehr und somit auch einfachere Integration in bestehende Netze. Diese beiden Aspekte werden in den Kapiteln 2 bzw. 4 im Detail betrachtet. Zusätzliche Details zu den Vorteilen von CV QKD können beispielsweise dem Review [2] entnommen werden.

Auf der anderen Seite ist CV QKD noch sehr jung und dadurch zum derzeitigen Zeitpunkt weniger ausgereift als DV QKD. So gibt es beispielsweise das BB84 Protokoll bereits seit 1984, während das GG02 Protokoll erst 2002 entwickelt wurde. Dies führt dazu, dass trotz der theoretischen Überlegenheit von CV QKD insbesondere bei hohen Distanzen aktuell in praktischen Umsetzungen geringere Reichweiten und SKRs als bei DV QKD erreicht werden. Ursachen dafür sind oft kleinere Wiederholungsraten [7] oder Rauschen bei hohen Wiederholungsraten und eine geringe Effizienz im Post-Processing [2]. Zusätzlich sind viele der notwendigen Sicherheitsbeweise noch jung (für GG02 Protokoll ca. 2009) oder z.T. für manche CV Protokolle noch ausstehend [2] und aktuell findet ein grundlegender Generationenwechsel von TLO zu LLO statt [2],[6].

## Fazit

Da sich die etablierten QKD Hersteller wie ID Quantique oder Toshiba bisher hauptsächlich auf das gut verstandene DV QKD konzentriert haben, sind viele der realisierten CV QKD Systeme eher experimentell. Allerdings ist inzwischen auch Huawei in die Forschung an CV QKD eingestiegen [16], [17] und es gibt auch einige junge europäische Start-Ups in dem Feld, beispielsweise LuxQuanta in Spanien [18] und KEEQuant in Deutschland [19]. Es scheint, als ob der aktuelle Fokus bei CV QKD auf kurzreichweitigen Metroverbindungen liegt und diese durch Verwendung von kommerziellen Bauteilen, PICs und Koexistenz mit klassischem Datenverkehr kosteneffizient realisiert werden sollen. Es bleibt also noch abzuwarten, ob zukünftig auch langreichweitige CV QKD Systeme verfügbar sein werden, oder ob für diese Anwendungen DV QKD oder auch Twin-Field QKD verwendet werden muss.

## 2. Twin-Field QKD

Twin-Field (TF) QKD ist ein erst 2018 von Toshiba [20] entwickeltes *Prepare & Measure* (PM) QKD Verfahren, bei dem Quanteninformationen in der Phase von Laserpulsen codiert und an einem zentralen Relay verglichen werden. Da es Reichweiten bis über 1000 km ermöglicht [21], wurde es sehr viel untersucht und es liegen trotz seines geringen Alters auch bereits alle nötigen Sicherheitsbeweise vor [22].

Zunächst wird das TF Protokoll detailliert vorgestellt, bevor auf Aspekte der Realisierung eingegangen wird. Abschließend werden Vor- und Nachteile dieser neuen Technologie thematisiert und ein (kommerzieller) Ausblick gegeben.

### Protokoll

Bei TF QKD präparieren Alice und Bob phasenmodulierte Zustände und schicken diese zu einem zentralen Relay, wo es zu Interferenz kommt. Ein typisches Setup ist in *Abbildung 2* veranschaulicht. Es werden keine Einzelphotonenquellen, sondern abgeschwächte Laserpulse mit *Decoy States* zur Vermeidung von Seitenkanalangriffen verwendet. Die Nutzer entscheiden daher zufällig bei der Zustandspräparation, ob sie einen Signal- oder Decoy-Zustand präparieren wollen und wählen entsprechend die Signal- oder eine der Decoy-Intensitäten. In beiden Fällen erfolgt eine Phasenmodulation der Zustände, wobei bei den meisten TF Protokollen, zusätzlich zu Beiträgen z.B. durch das zu encodierende Bit, ein Teil der Phase durch sogenannte *Phaseslices* gegeben ist. Hierbei wird die Phase zwischen 0 und  $2\pi$  in äquidistante Abschnitte aufgeteilt, einer dieser Abschnitte zufällig ausgewählt und ein beliebiger Wert innerhalb der gewählten Phaseslice als zusätzlicher Beitrag zur Gesamtphase verwendet. Am Relay kommt es zu einer Ein-Photonen-Interferenz an einem Strahlteiler, wodurch der gesamte TF QKD Aufbau effektiv einem sehr großem *Mach-Zehnder Interferometer* (MZI) entspricht. Wenn nun zwei Zustände z.B. mit identischer Gesamtphase gleichzeitig ankommen, so liegt ein sog. Twin-Field vor und es kommt zu einem Interferenzeffekt, wodurch nur einer der beiden nachfolgenden Photonendetektoren ausschlägt. Das Relay teilt öffentlich mit, welche Detektoren ausgeschlagen haben und die Nutzer veröffentlichen die verwendeten Intensitäten und Basen. Dadurch können im Twin-Field Fall (falls auch jeweils die Signal-Intensität und gleiche Basen verwendet wurden), Alice und Bob ausgehend von dem Wissen der Phase ihres eigenen Zustandes, die Phase des anderen erschließen und somit einen geheimen Schlüssel erzeugen. So setzt sich beispielsweise im originalen TF Protokoll die Gesamtphase der Zustände aus Beiträgen von Basis, Bit und Phaseslice zusammen. Wenn nun das Relay ein Twin-Field meldet, so liegt automatisch bei beiden Nutzern das gleiche Bit vor, falls die gleiche Phaseslice und auch die gleiche Basis zufällig gewählt wurden. Die anderen Ereignisse dienen entweder der QBER bzw. Decoy Analyse oder werden verworfen. Eine detaillierte bzw. anschauliche Erklärung des TF Protokolls kann beispielsweise in dem Review Paper [2] oder auf der Website [23] gefunden werden.

Da das Relay nur einen Vergleich der Zustände ausführt, muss ihm nicht vertraut werden und es handelt sich bei TF QKD um ein *Measurement-Device Independent* (MDI) QKD Protokoll. Hier ist allerdings anzumerken, dass sich diese Art der MDI QKD stark von anderen MDI Ansätzen unterscheidet [24], die normalerweise auf einer anderen Interferenz (Hong–Ou–Mandel Effekt) am zentralen Relay basieren und daher fundamental mehr als einen Strahlteiler und zwei Detektoren benötigen.

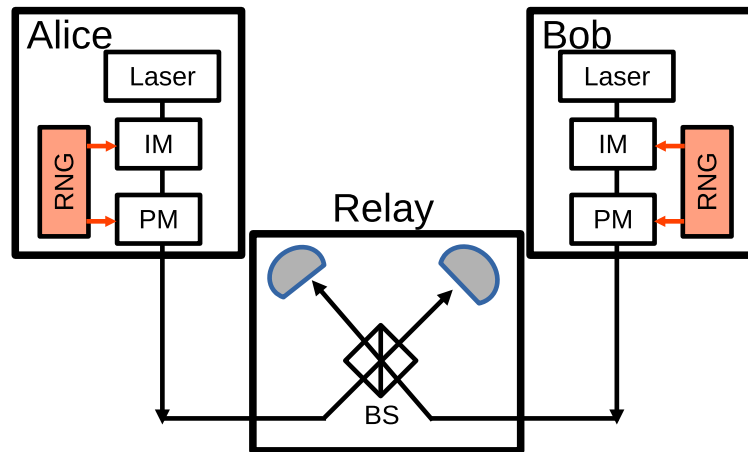


Abbildung 2: **Typisches TF QKD Setup.** Die Nutzer Alice und Bob verfügen je über einen Laser der mittels Intensitäts (IM)- & Phasenmodulatoren (PM) und Random Number Generator (RNG) modulierte Pulse erzeugt, die zu einem Relay geschickt werden und dort an einem Strahlteiler (BS) interferieren.

Ausgehend von dem ursprünglichen TF Protokoll [20] wurden verschiedene Variationen mit speziellen Eigenschaften entwickelt. Das aktuell mit Abstand meist genutzte TF Protokoll ist das sogenannte *Sending-Not-Sending* (SNS) Protokoll [25], bei dem der Schlüssel nicht aus den interferierenden Zuständen erhalten wird, sondern diese nur zur Überwachung dienen. Es ist in diesem Protokoll möglich, dass Alice bzw. Bob einen Zustand, der in der Signal-Intensität präpariert werden würde, gar nicht senden. Alice (Bob) kodieren dann z.B. das Bit 1 (0) dadurch, einen Zustand zu senden und das Bit 0 (1) darin, keinen Zustand zu senden. Meldet nun das Relay, dass genau ein Photon detektiert wurde, so liegt entweder bei beiden das gleiche Bit vor (falls nur einer der beiden einen Zustand gesendet hat) bzw. entgegengesetzte Bits (falls beide einen Zustand im TF gesendet haben). Sendet beispielsweise Alice einen Zustand und Bob keinen, so liegt bei beiden das Bit 1 vor. Durch geschickte Auswahl der Wahrscheinlichkeiten tritt der ungewollte Fall mit entgegengesetzten Bits seltener auf und wird in der Fehlerkorrektur behoben. Die Sicherheit ist in diesem Ansatz dadurch gegeben, dass nur bekannt gegeben wird, ob eine Signal-Intensität präpariert werden sollte (und nicht ob dies auch tatsächlich gemacht wurde) und die Messung erst nach dem Strahlteiler erfolgt. Da Interferenz somit nur für die Überwachung der Schlüsselerzeugung benötigt wird, ist dieses Protokoll effizienter bei großen Reichweiten, wo die Interferenz schwieriger ist. Für kürzere Reichweiten versprechen z.B. das *Four-Phase* Protokoll höhere Schlüsselraten, indem auf das Phaseslicing verzichtet wird und dadurch die Effizienz steigt [22].

### Realisierung

Die Realisierung von Interferenz zwischen Signalen, die Hunderte von Kilometer entfernt erzeugt werden und davor durch Glasfasern propagieren, ist technisch sehr aufwändig. Die beiden wichtigsten Ursachen für die zu vermeidenden relativen Phasenfluktuationen zwischen den am Relay ankommenden Zuständen sind [2]:

1. Phasenfluktuationen, hervorgerufen durch Wellenlängenfluktuationen der Laser bei Alice/Bob
2. ein Phasendrift verursacht bei der Propagation durch die Glasfaser

Die **Wellenlängenfluktuationen** der Laser können zum einen durch die Verwendung von (ultra) frequenzstabilen Lasern mit geringer Linienbreite stark reduziert werden. So wurde beispielsweise in [26] demonstriert, dass die Verwendung von lokalen Frequenzreferenzen eine gegenseitige Frequenzstabilisierung der Laser unnötig machen kann und in [27] musste nur einmal pro Stunde der Frequenzdrift zwischen den Lasern korrigiert werden. Für die meisten Realisierungen wird allerdings eine kontinuierliche Frequenzstabilisierung der Laser von Alice und Bob benötigt, indem diese mittels

eines Referenzsignals zueinander oder zu einer gemeinsamen Quelle am Relay geregelt werden [28]. Dafür werden normalerweise entweder *Optical Phase Locked Loops* (OPLL) verwendet, wo ein komplexes Feedback System die Userlaser an die Referenz anpasst, oder auch *Optical Injection Locking*, wo das Einspeisen der Referenz in die *Laser Cavity* bei den Usern automatisch die Wellenlänge synchronisiert. Es sei hier angemerkt, dass das notwendige Referenzsignal dafür sogar verstärkt werden kann, allerdings steigt dadurch die Komplexität des Gesamtsystems und es wird zusätzliches Rauschen verursacht [22].

Auch für die **Kompensation des Phasendriffs** im Quantenkanal, der beispielsweise durch Längenveränderungen aufgrund von Temperaturänderungen im Tag-Nacht-Zyklus hervorgerufen wird, existieren verschiedene Lösungsansätze [24]. In einigen Realisierungen von TF QKD wird ein als *Sagnac Loop* bekanntes passives Verfahren basierend auf gegenläufigen Pulsen verwendet, so beispielsweise in [29]. In den meisten Fällen wird aber ein (starkes) zeitgemultiplextes Referenzsignal parallel zum Quantensignal verwendet, um den Phasendrift bestimmen und anschließend korrigieren zu können. Der so bestimmte Phasendrift dient dann entweder als Feedback Signal zur Steuerung von Phasenmodulatoren in Echtzeit, kann aber auch stattdessen im Post-Processing berücksichtigt werden [29].

Insbesondere bei sehr großen Reichweiten tritt allerdings ein Dilemma auf: Es werden mehr bzw. stärkere Referenzsignale benötigt, um den Phasendrift verlässlich zu bestimmen, was aber auch mehr Störungen im Quantensignal erzeugt, das aufgrund der großen Distanzen ohnehin extrem schwach ist. Außerdem wird durch das zeitgemultiplexte Referenzsignal die effektive Wiederholungsrate und somit auch die Schlüsselrate reduziert. Eine Lösung dafür bietet ein als **Dual Band Stabilization Technique** bezeichnetes Verfahren von Toshiba [31], das aus der Frequenzmetrologie stammt [32]. Hierbei wird ein zusätzliches, wellenlängengemultiplextes Referenzsignal verwendet. Das Relay verteilt dann zwei Referenzsignale unterschiedlicher Wellenlänge und Intensität zu Alice und Bob. Das hellere Referenzsignal einer anderen Wellenlänge dient nur zur Bestimmung des Phasendriffs, während das schwächere, das die gleiche Wellenlänge wie das Quantensignals hat, zur Frequenzstabilisierung der Laser und zur Feinbestimmung des Phasendriffs dient. Auch wenn die Verwendung einer zusätzlichen Wellenlänge eine erhöhte Komplexität mit sich bringt, lassen sich durch dieses Verfahren extrem hohe Reichweiten realisieren [21]. Es sei hier außerdem angemerkt, dass dieses Verfahren zusätzlich zur Phasendriftbestimmung direkt eine kontinuierliche Frequenzstabilisierung der Laser bei Alice und Bob ermöglicht und in Feldversuchen reduzierte Anforderungen an die Laser demonstriert wurde [33].

Jenseits von den besonderen Anforderungen der TF QKD an die Phasenstabilität des Systems müssen auch hier, vergleichbar zum BB84 Protokoll, Einzelphotonen verlässlich detektiert werden, was insbesondere bei großen Distanzen sehr aufwendig ist und normalerweise *Superconducting Nanowire Single-Photon Detectors* (SNSPDs) nötig macht. Analog gilt es bei den großen Distanzen Rauschen zu vermeiden, wofür Filter, optimierte Kanalbelegungen oder zeitliche Synchronisation von Signal und Detektion verwendet werden können [27]. Außerdem setzt die erfolgreiche Interferenz der Zustände am Relay eine Kompensation von Polarisations- und Ankunftszeitschwankungen voraus, was normalerweise in Echtzeit über Feedback-Schleifen realisiert wird. Dadurch wird beispielsweise in [27] und [33] eine Synchronisation der Ankunftszeiten von ca. 10 ps erreicht.

*Tabelle 2* gibt einen Überblick über aktuelle TF QKD Experimente bzw. Testbeds. Dabei wird in den Anmerkungen beschrieben, wie die jeweiligen Realisierungen mit den Wellenlängenfluktuationen und dem Phasendrift umgehen. Außerdem wird hervorgehoben, falls ein anderes Protokoll als SNS TF QKD vorliegt oder es sich um eine praxisnahe Realisierung handelt.

Quelle	Jahr	SKR	Reichweite (Dämpfung)	Wiederholungsrate
<b>Anmerkungen</b>				
[27]	2021	3.4 bps	511 km 89 dB	100 MHz
Aufgrund lokaler Frequenzreferenzen nur 1x/h Frequenzsynchronisation zwischen den Teilnehmern nötig, Phasendriftkorrektur im Post-Processing mit zeitgemultiplexer Referenz; Glasfaserbündel zwischen zwei Städten				
[22]	2022	14 mbps	834 km	1.6 GHz
OPLL, Phasendriftkorrektur durch Feedback mit zeitgemultiplexer Referenz; Four-Phase Protokoll				
[21]	2023	3.4 mbps <sup>2</sup>	1002 km 157 dB	350 MHz
Dual Band Stabilization Technique mit Post-Processing; aktueller TF QKD Reichweitenrekord via top-end Laser, Faser und Detektor				
[26]	2024	9.7 bps	502km 84 dB	100 MHz
Lokale Frequenzreferenzen, Phasendriftkorrektur im Post-Processing mit zeitgemultiplexer Referenz				
[28]	2024	8.5 bps	75 dB	1 GHz
Optical Injection Locking, Phasendriftkorrektur durch Feedback mit zeitgemultiplexer Referenz; photonische Integration				
[33]	2024	110 bps	254 km 56 dB	500 MHz
Dual Band Stabilization Technique mit Feedback; Toshiba Feldtest; asymmetrische Linklängen; Avalanche-Photodioden				

Tabelle 2: Übersicht zu aktuellen TF QKD Experimenten und Testbeds

### Vor- und Nachteile

Der größte Vorteil von TF QKD ist die extrem hohe erreichbare Reichweite bzw. die hohe Schlüsselrate bei hohen Reichweiten im Vergleich zu anderen QKD Protokollen. Beispielsweise wurde in [21] erstmals in glasfaserbasierter QKD eine Reichweite von >1000 km demonstriert. Auch wenn diese Demonstration extrem leistungsstarkes Equipment verwendet hat und bei der größten Reichweite keine Finite-Size Effekte berücksichtigt wurden, hat dieses Experiment sehr deutlich die Kapazität von TF QKD für langreichweitige QKD Verbindungen demonstriert. Auf der anderen Seite ermöglicht es TF QKD aber auch bei Distanzen, die mit etablierteren QKD Protokollen erreicht werden können, deutlich höhere Schlüsselraten zu erreichen [22]. So wird beispielsweise in [22] mit einem TF QKD Verfahren über 500 km eine SKR von über 300 bps erreicht, während die extrem langreichweitige BB84 Realisierung in [34] über eine Glasfaserdistanz von etwas mehr als 400 km nur 6.5 bps erreicht. Der Grund dafür ist, dass bei TF QKD das Relay, an dem die Interferenz der Signale stattfindet, quasi die Reichweite verdoppelt [2]. Bei Protokollen ohne ein solches Relay wie BB84 oder auch CV QKD skaliert die maximal theoretisch erreichbare Schlüsselrate als Funktion der Kanaltransmission linear (Kanaltransmission skaliert exponentiell zur Distanz). Dies ist in der Literatur als Pirandola-Laurenza-Ottaviani-Banchi (**PLOB**) Grenze bekannt. Im Gegensatz dazu liegt bei TF QKD ein Kanal mit einem Repeater/Relay vor und die maximal theoretisch erreichbare Schlüsselrate skaliert mit der Wurzel der Kanaltransmission, wodurch zwar bei sehr kleinen Distanzen geringere Schlüsselraten resultieren, aber dafür höhere Reichweiten bzw. Schlüsselraten bei großen Distanzen erreicht werden können. Dies ist in *Abbildung 3* veranschaulicht, wo die PLOB und die 1-Repeater Grenze gezeigt werden, neben theoretisch erreichbaren SKRs bei idealen BB84 bzw. TF Realisierungen und einigen experimentellen

<sup>2</sup> Ohne Finite-Size Effekte

SKRs. Somit stellt TF QKD aktuell die einzige realisierbare Möglichkeit dar, die fundamentale PLOB Grenze zu überschreiten, zumindest solange es noch keine funktionierenden Quantenrepeater gibt. Beispielsweise wird in [22] die PLOB Grenze um mehr als zwei Größenordnungen überschritten. Hier sei angemerkt, dass die Verwendung eines zentralen Relays in einem QKD Protokoll nicht automatisch dazu führt, dass die PLOB Grenze überschritten wird. Beispielsweise haben andere MDI QKD Protokolle, die ebenfalls ein Relay aufweisen, bedingt durch die verwendete Interferenz auch nur eine lineare Skalierung mit der Kanaltransmission [2].

Die verwendete Relay Architektur vereinfacht außerdem die Realisierung von Multiuser Konfigurationen [35] und es ist auch möglich, die notwendige Komplexität bei den Nutzern zu reduzieren [28]: So werden dort beispielsweise keine Detektoren bei den Nutzern gebraucht, die oftmals den komplexesten Teil bei QKD darstellen.

Der größte Nachteil von TF QKD ist der hohe Aufwand, die Interferenz zwischen Signalen, die Hunderte von Kilometern entfernt erzeugt werden und davor durch Glasfasern propagieren, zu realisieren. Aktuell ist es außerdem oft sehr schwierig, Interferenz im Fall von asymmetrischen Linklängen zwischen Relay und Nutzern zu ermöglichen. Tritt dieser Fall auf, so werden meist zusätzliche Faserspulen verwendet [33], was die Flexibilität und SKR reduziert. Die oben beschriebenen Verfahren zur Phasenkorrektur benötigen oft zusätzliche Fasern und im Fall von großen Reichweiten sind *Dark Fibers* für den Quantenkanal eigentlich unabdingbar. Durch die Verwendung von Phaseslices ergibt sich außerdem ein zusätzlicher QBER Beitrag und oft ist die totale Effizienz zwischen gesendeten und verwendbaren Zuständen sehr gering [27].

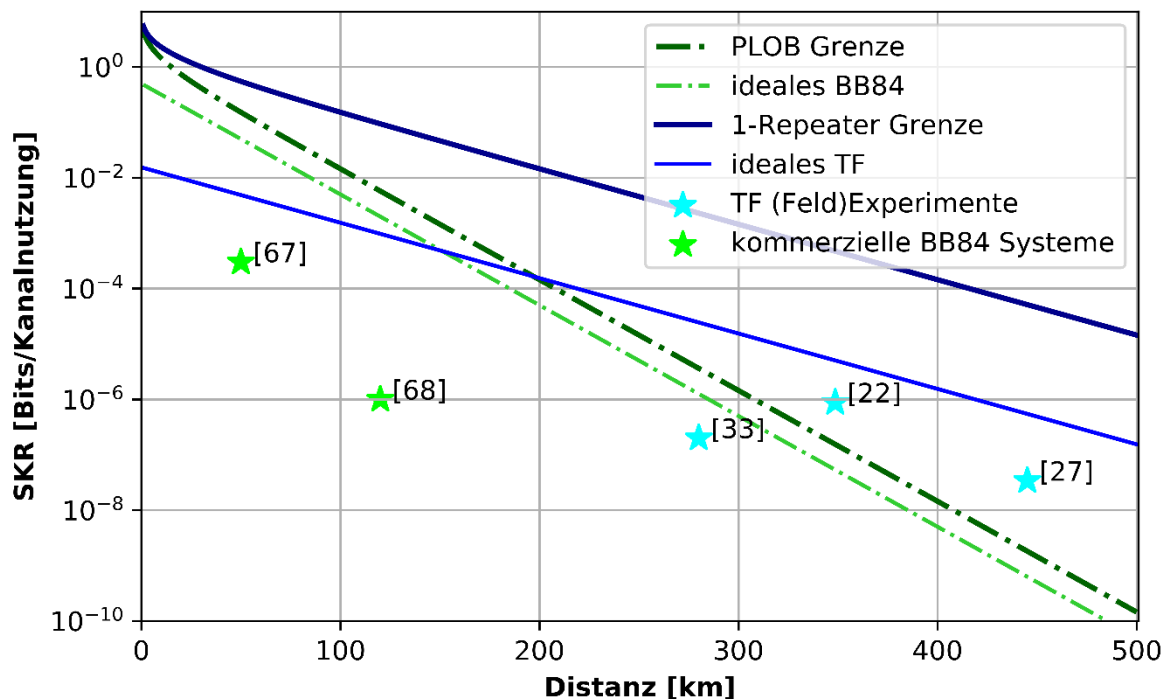


Abbildung 3: **Typische experimentelle SKR Werte und theoretische Grenzen für TF QKD im Vergleich zu BB84.** Während die maximale SKR bei BB84 der PLOB Grenze folgt, weist TF QKD die gleiche Skalierung wie die höhere 1-Repeater Grenze auf [2]. Zur Orientierung sind auch SKRs aus tatsächlichen Realisierungen in (Feld)-Experimenten bzw. kommerziellen Systemen gezeigt. Bei einer angenommenen Dämpfung von 0.2dB/km kann eine ideale TF Realisierung eine ideale BB84 Realisierung/die PLOB Grenze bei 150/200km übertreffen.

## Fazit

Die praktische Realisierung der phasenbasierten TF QKD stellt einen weiteren Schritt in Richtung Quanteninternet dar, da hier erstmals demonstriert wurde, dass die sehr komplizierte zuverlässige Übertragung der Phase über große Reichweiten technisch möglich ist.

Auch wenn aktuell noch keine kommerziellen Geräte verfügbar sind, wurde die Realisierung dieser Technologie bereits wiederholt im freien Feld demonstriert [26], [31], dieses Jahr sogar von Toshiba und GÉANT in einer kommerziellen Telekommunikationsumgebung [33]. Der wichtigste kommerzielle Spieler ist bisher Toshiba, aber auch China forscht sehr intensiv an diesem Protokoll. In Experimenten wurde außerdem die Multiuser Tauglichkeit demonstriert [29], [35] und erste Experimente in die Richtung der photonischer Integration sind bereits erfolgt [28]. Es ist daher sehr wichtig, dieses sehr vielversprechende Verfahren für langreichweitige Backbone Verbindungen genau im Auge zu behalten.

### 3. Multipoint QKD

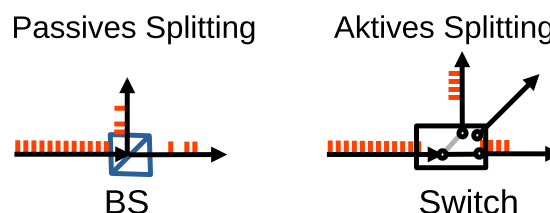
Bisher sind QKD-Netzwerke meist über einzelne *Point-to-Point* (P2P) Verbindungen realisiert, da die bisher gängigen PM Protokolle nur für eine P2P-Kommunikation zwischen zwei Knoten konzipiert sind. Die herkömmlichen P2P-Verbindungen können zwar über *Trusted Nodes* aneinandergereiht zu einem einfachen QKD-Netz erweitert werden, allerdings bringen Multipoint-Netzwerke mit Trusted Nodes Sicherheitsnachteile mit sich, da die Information an den Nodes kurzzeitig unverschlüsselt vorliegen muss, um für die nächste P2P-Strecke erneut verschlüsselt zu werden. Auf eine Verringerung der Anzahl der Trusted Nodes zielt der Ansatz der *Partially Trusted Nodes* ab. In [36] können in Trusted-Node-basierten Netzwerken MDI-Empfänger an *Untrusted Nodes* bzw. MDI-Transmitter an Trusted Nodes eingesetzt werden, um so die Sicherheit (z.B. gegen *Side-Channel Angriffe* gegen Detektoren) zu erhöhen. Die Untrusted Nodes bieten dabei keine Angriffsmöglichkeit, da sie durch das MDI-Schema quantensicher sind. Um aber ein reales, einfach skalierbares Netzwerk mit möglichst wenigen Trusted Nodes aufzubauen, müssen nicht nur viele Nutzer unterstützt werden (Multiuser Netzwerke), wodurch die Anzahl der einzelnen P2P Verbindungen sehr schnell skalieren würde, sondern es müssen auch *Point-zu-Multipoint* (P2MP) Verbindungen unterstützt werden, wie sie beispielsweise in einer Stern- oder Baum-Topologie zu finden sind [37].

Für Multipoint QKD gibt es verschiedene Ansätze zur Realisierung, die sich in folgende Kategorien gliedern lassen:

- Hardware-basierte Erweiterungen der P2P-Protokolle: Optisches *Splitting* & *Switching*, *Wavelength Division Multiplexing* (WDM)
- Protokoll-basierte Abänderungen geeigneter Protokolle: Multiuser TF QKD, Multiuser verschränkungs-basierte QKD, Multiuser CV QKD, Multiuser *Differential Phase Shift* (DPS) QKD

#### Hardware-basierte Erweiterungen der P2P-Protokolle

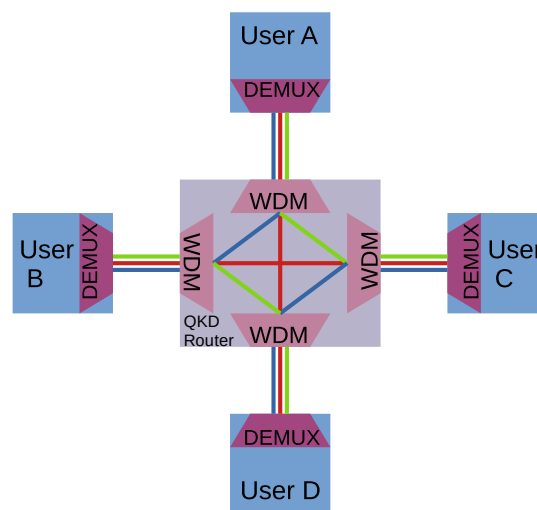
Die einfachste Möglichkeit, um die Kommunikation zwischen mehreren Teilnehmern in einem Netzwerk zu ermöglichen, ist die des optischen passiven Splittings oder des aktiven Switchings [38], um P2P-Systeme zu einem Netzwerk zu erweitern und die Anzahl der Trusted Nodes zu verringern. Wie in *Abbildung 4* veranschaulicht, werden dabei die QKD Signale entweder zufällig oder gesteuert auf mehrere Faserwege aufgeteilt. Dies bringt allerdings immer eine Reduktion der SKR im Vergleich zur P2P Verbindung mit sich, da zum einen durch die zusätzlichen Bauteile die Dämpfung erhöht wird, und andererseits die ursprüngliche Kanalkapazität aufgeteilt wird.



*Abbildung 4: Vergleich von passivem und aktivem Splitting.* Bei passivem Splitting werden üblicherweise Strahlteiler (BS) eingesetzt.



Eine weitere Technik zum Splitting ist die des Wellenlängenmultiplexings. Dabei werden verschiedene Wellenlängen für die Kommunikation zwischen verschiedenen Teilnehmern genutzt, wobei sie mittels WDM zusammengeführt und mit dem Demultiplexer (DEMUX) wieder einzeln aufgesplittet werden. Auch hier gibt es zusätzliche Einfügedämpfung. So wurden schon um 2010 herum QKD-Netzwerke auf diese Weise realisiert. In einem Feld-Experiment [39] wurde beispielsweise eine Sterntopologie mit vier Nutzern durch wellenlängenbasiertes Routing des in der Mitte befindlichen Routers realisiert, wie *Abbildung 5* zeigt. Dabei findet jeder Schlüsselaustausch mit den jeweils drei Partnern auf einer anderen Wellenlänge statt. Nachteil dieser Methode ist das Intraband-Übersprechen, verursacht durch die anderen Laser derselben Wellenlänge, welches sich negativ auf die SKR auswirken wird. Dafür kann auf Trusted Nodes verzichtet werden und das Verfahren ist theoretisch weiter skalierbar.



*Abbildung 5: WDM 4-Nutzer-Star-Topologie mit drei verschiedenen Wellenlängen (blau, rot, grün) [39].*

Verwandt dazu stellt [40] in einer Sterntopologie die Reduktion der verwendeten Wellenlängen anhand von fünf Knoten mit nur zwei verwendeten Wellenlängen dar. Dabei kann auf derselben Wellenlänge gesendet und empfangen werden, wodurch eine Wellenlängenreduktion zustande kommt. Es wird fest vorgeschrieben, welche Knoten miteinander auf welcher Wellenlänge senden/empfangen dürfen (siehe *Abbildung 6*): z. B. kann Knoten A auf Wellenlänge  $\lambda_1$  an B und  $\lambda_2$  an C senden, während A auf  $\lambda_2$  von D und auf  $\lambda_1$  von E gleichzeitig empfangen kann. Es kann also nur auf zwei Wellenlängen zu zwei bestimmten Partnern gesendet werden, während man bei den beiden anderen Partnern darauf angewiesen ist, dass der andere Teilnehmer sendet. Wie beim vorhergehenden Netzwerk ist eine gleichzeitige Schlüsselerzeugung zwischen jeden zwei Knoten möglich. Hierfür werden als Multiplexer ein 3-Port Zirkulator mit zwei WDMs und als Demultiplexer ein WDM mit zwei 3-Port-Zirkulatoren eingesetzt. Dabei besteht der 5-Port QKD Router aus fünf solchen (De-)Multiplexern, die die zwei Wellenlängen auf vier Verbindungen aufteilen/zusammenführen. Das Netzwerk ist grundsätzlich um zusätzliche Teilnehmer erweiterbar, indem WDMs mit  $N$ -fachen Wellenlängen und  $N$  Zirkulatoren an den neuen Knoten aufgebaut bzw. an den alten Knoten erweitert werden. Dabei soll das Interband-Übersprechen durch schmalbandige Filter unterdrückt werden können und so selbst bei vier zusätzlichen Komponenten vernachlässigbare Verluste durch Intraband-Übersprechen und Einfügedämpfung generiert werden können.

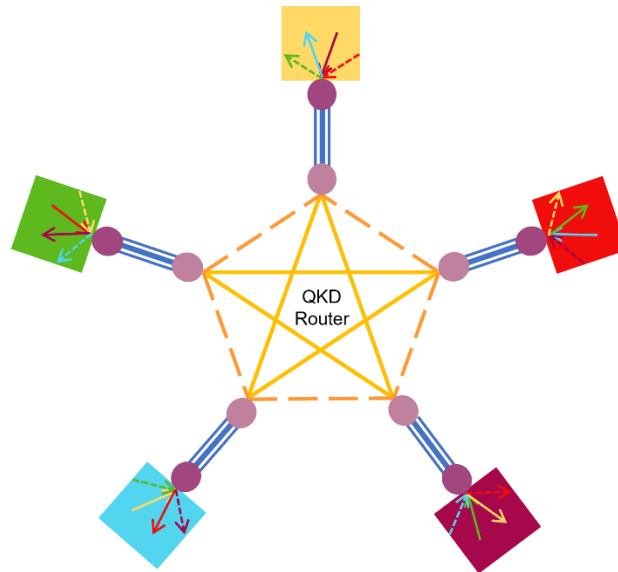


Abbildung 6: **Wellenlängen-einsparende 5-Nutzer Sterntopologie** [40]. Die Kommunikation zwischen zwei Nutzern ist farblich gekennzeichnet; gestrichelte bzw. durchgezogene Linien stellen die zwei verschiedenen Wellenlängen dar; die (De-)Multiplexer als Zirkulatoren mit WDMs sind als purpurne Kreise gekennzeichnet.

[41] kehrt den oft auftretenden P2MP Downstream-Ansatz eines Senders zu vielen Empfängern mit jeweils einzelnen SPDs um in einen Upstream-Ansatz von mehreren Sendern zu einem gemeinsamen Empfänger, wie *Abbildung 7* veranschaulicht. Im Unterschied zu MDI QKD, muss bei diesem Ansatz aber dem Empfänger-Knoten intrinsisch vertraut werden. Hier soll ein einziger SPD mit bis zu 64 Empfängern (@ 20 km) bei vernachlässigbarem Übersprechen durch passive optische Splitter gemeinsam in einem phasen-codierten BB84-Protokoll mit aufeinanderfolgenden Zeitschlitz für jeden Teilnehmer genutzt werden können. Im Vergleich zum Downstream-Ansatz fallen viele Probleme weg, wie die vielen benötigten SPDs bei den Nutzern, sowie die erforderte gleich hohe Geschwindigkeit der Empfänger relativ zum Sender, sodass die hohe Empfängerbandbreite nun gemeinsam effizienter genutzt werden kann. Durch die verringerte Geschwindigkeit können vereinfachte, kostengünstige Sender eingesetzt werden. Allerdings muss jeder Nutzer die Systemschwankungen individuell vorkompensieren, da es keine aktive Stabilisierung durch den Empfänger gibt. Bei weniger Benutzern ergibt sich ein Spielraum, um längere Faserdistanzen/ höhere Verluste zu ermöglichen. Die SKR kann durch die Verwendung von WDM mit geringeren Verlusten statt der passiven Splitter erhöht werden.

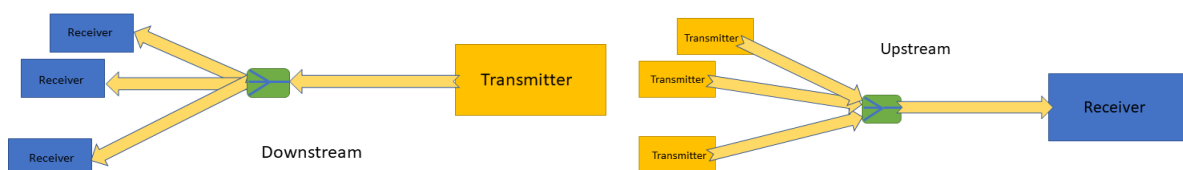


Abbildung 7: **Down-/Up-Stream Quantum Access Network** [41].

In [42] wird der theoretische Einsatz von aktiven Switches basierend auf der *Micro-Electro-Mechanical Systems* (MEMS) Technologie untersucht. Konkret wird ein rein optisch geschaltetes CV QKD Netzwerk simuliert, wobei sich die  $1 \times N$  Switches durch ihre besonderen Eigenschaften auszeichnen, wie schnelles Schalten, geringe Einfügedämpfung, geringes Übersprechen und somit hohe Datenraten ermöglichen. Allerdings treten ungleichmäßige Verluste an den Ports der Switches auf. Es können theoretisch auf 10/20 km 10/1 Mbps SKR bei einem  $1 \times 4/1 \times 12$  MEMS-Switch erreicht werden.

Für die dynamische Allokation von Quantenpfaden muss bei großen QKD-Netzen *Software-Defined Networking* (SDN) eingesetzt werden. In [43] wird SDN für optimales dynamisches Switching und Rerouting mittels kontrollierbaren *quantum Reconfigurable Optical Add Drop Multiplexern* (qROADMs)

für DV QKD eingesetzt. In [44] wird ein interoperables Netzwerk in Madrid flexibel durch SDN-basiertes Switching und *DenseWDM* (DWDM) für CV & DV QKD gesteuert. Hier kann durch dynamisches Routing auf verschiedenen Wellenlängen eine anpassbare Multiuser Architektur geschaffen werden. Besonders die QKD-Geräte von Huawei unterstützen Wellenlängen in einem breiten Bereich, sodass unterschiedliche QKD-Geräte Paarungen flexibel zwischen je fünf Sendern/Empfängern realisiert werden.

## Multiuser-Protokolle

Im Folgenden werden Multiuser Realisierungen basierend auf speziell dafür geeigneten Relay-basierten-Protokollen, wie z.B. dem eben vorgestellten TF-Protokoll (vgl. Kapitel 2), verschränkungs-basierten Protokollen, sowie weiteren (für Multiuser noch nicht gängigen) Protokollen z.B. CV (vgl. Kapitel 1) und DPS, die für Multiuser erweitert wurden, vorgestellt. Manche Protokolle sind noch recht theoretisch, doch es gibt auch bereits einige konkrete Realisierungen auf diesem Gebiet. Analog zu den hardware-basierten Ansätzen, können so beliebige P2P Verbindungen in einem Netzwerk realisiert werden, ohne dass man Trusted Nodes braucht. Zudem existieren auch QKD Protokolle, bei denen ein Schlüssel an mehrere Nutzer gleichzeitig verteilt wird. Diese Art der Protokolle sind als *Quantum Cryptographic Conference* oder auch als *Conference Key Agreement* bekannt.

### Multiuser TF-Protokoll

Das in *Kapitel 2* vorgestellte relaybasierte TF-Protokoll ist zwar für weite Distanzen geeignet, aber sollen mehrere Nutzer hinzugefügt werden, so stellen die hohen Anforderungen an die gemeinsame Phasenstabilisierung ein Problem dar, welches in der Literatur meist mit Sagnac-basierten Interferometern umgangen wird, welche auch asymmetrische Entfernungen zum Messterminal ermöglichen [45]:

So präsentiert [29] ein ringbasiertes Multiuser-Sagnac-Interferometer, das neben der Phasenstabilisierung auch einen asymmetrischen Aufbau ermöglicht, der für Multiuser typisch ist. Dies wird erreicht, indem entgegengesetzt durchlaufende Signale in einer bidirektionalen Schleife verwendet werden. So kann eine aktive Phasenstabilisierung vermieden werden, die normalerweise bei TF QKD angewendet werden muss. Bei der beschriebenen Realisierung teilen sich alle drei Benutzer die gleiche Laserquelle und SPDs am zentralen Knoten. Die beiden kommunizierenden Nutzer modulieren je eines der sich im und gegen den Uhrzeigersinn bewegendem Signale mit zufälliger Phase und (Decoy) Intensitäten. Der zentrale Knoten misst mit zwei SPDs und veröffentlicht mit anschließender Distillation. Die gleichzeitige Kommunikation zwischen verschiedenen Nutzern ist per Time-Multiplexing möglich und eine Kollision der umlaufenden Signale wird durch unterschiedliche Faserverlängerungen bei den Nutzern vermieden. Neue Nutzer können einfach hinzugefügt werden, indem nur die Faserlänge kalibriert wird und keine weiteren Änderungen an der Hardware vorgenommen werden müssen.

Einen anderen Ansatz verfolgt [35], wo ein  $2 \times N$  TF QKD-Netz in Stern-Topologie basierend auf Polarisations-, Wellenlängen-, und Zeitmultiplexing (TDM) ausgehend von dem bereits im Kapitel 2 vorgestellten SNS TF QKD Protokoll realisiert wird. Der verwendete Aufbau ist in *Abbildung 8* visualisiert. Das Netzwerk unterstützt *Plug-and-Play*, sodass der Schlüsselaustausch sofort beginnen kann, wenn das Client-Gerät an das Ende der Faser angeschlossen und das Signal synchronisiert worden ist. Indem eine Sagnac-basierte Architektur eingesetzt wird, kann auf aufwendige aktive Frequenz- und Phasenstabilisierung verzichtet werden. Während am zentralen Knoten ein Laser (L) pro Alice und ein Paar SPDs verbaut sind, besitzen die gepaarten Nutzer nur einen Strahlteiler mit einer Fotodiode (PD) zur Messung von Triggersignalen für die Synchronisation und Phasen (PM)- und

Intensitätsmodulatoren (IM) für das TF QKD Protokoll. Durch das Polarisationsmultiplexing (horizontal H, vertikal V) können die zwei Alices unabhängig voneinander jeweils mit einem Bob (der aus mehreren Bobs bestehen kann durch WDM) gleichzeitig Schlüssel über jeweils im und gegen den Uhrzeigersinn laufende Signale erzeugen. Dies wird erreicht indem im Relay verschiedene Strahlteiler (BS) und polarisierende Strahlteiler (PBS) eingesetzt werden. Das Schema ist leicht mit zusätzlichen Bobs skalierbar und gilt als sehr stabil. Zudem dürfte es durch den reduzierten Hardwareanspruch der Teilnehmer leicht kommerziell umsetzbar sein.

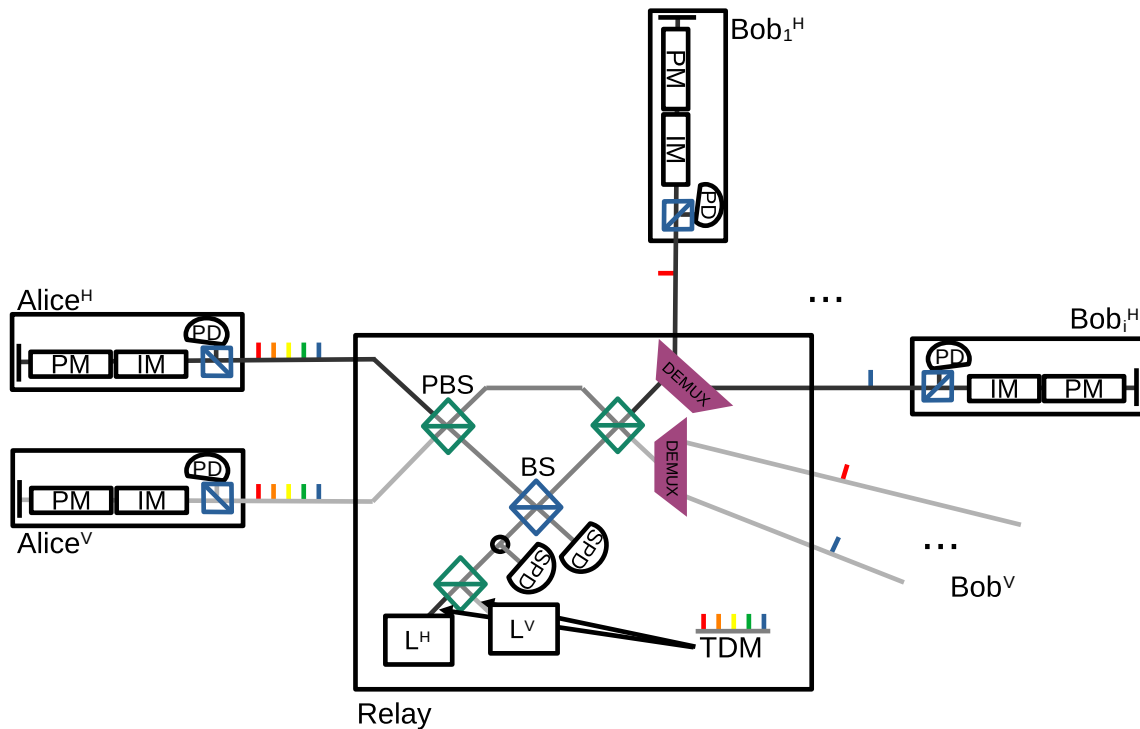


Abbildung 8:  $2 \times N$  TF QKD Realisierung [35]. Details und Abkürzungen sind im Text erklärt.

### Verschränkungsbasierte Protokolle

Insbesondere QKD Protokolle die auf einem zentralen Relay basieren, eignen sich sehr gut für die Erzeugung von Multiuser QKD Netzwerken: So auch die verschränkungsbasierten Protokolle, bei denen am zentralen Relay durch *Spontaneous Parametric Down-Conversion* (SPDC) verschränkte Photonenpaare erzeugt werden. Die Teilnehmer sind paarweise an das zentrale Terminal angebunden und erzeugen ihren eigenen geheimen Schlüssel.

Diese Protokolle orientieren sich an einem System mit drei Terminals. Dabei gibt es ein zentrales Terminal, das die verschränkten Photonen generiert und damit manchmal auch die Kontrolle über den Verbindungsaufbau der Teilnehmer innehat [46]. Ein *Greenberger-Horne-Zeilinger* (GHZ) Zustand ist ein verschränkter Vielteilchenzustand, der sich für bisher theoretische Multiuser-Realisierungen, sogar mit Multiknoten anbietet. So könnten  $N$  Nutzer gleichzeitig durch Messung einen gemeinsamen Schlüssel erhalten. [47] zeigt, dass simulativ Reichweiten über das MDI-Schema einzeln von 280 km durch *Entanglement Swapping* erreicht werden könnten.

Paarweise verschränkte Photonen können auch wellenlängen-selektiv an verschiedene Nutzer verteilt werden, wie in [48] beschrieben und in *Abbildung 9* dargestellt. Ein DWDM (De)Multiplexing-Schema mit Strahlteilern teilt dort passiv verschränkte Photonen auf 16 Wellenlängen gemäß dem ITU-Frequenzraster für 8 Nutzer inkl. Premiumverbindungen auf. In [49] wird eine aktive Aufteilung von

verschränkten Photonen auf Wellenlängenpaare durch einen softwaredefinierten Switch genauer behandelt und ein Switching-Algorithmus entworfen, was die Aufnahme von neuen Nutzern erleichtert. [50] wendet zusätzlich zu DWDM *Space Division Multiplexing* (SDM) an, um verschränkungs-basierte Time-Energy HD QKD (vgl. Kapitel 7). zwischen 40 Nutzern zu realisieren.

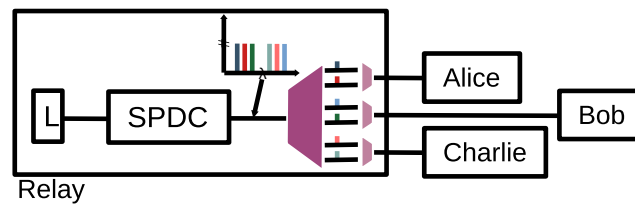


Abbildung 9: *Schematische Darstellung eines passiven QKD-Netzwerks basierend auf Verschränkung* [48]. Am zentralen Relay erzeugt der Output eines Lasers (L) in einem Kristall über den SPDC Prozess verschränkte Photonenpaare (visualisiert durch ähnliche Farben im gezeigten Spektrum). Diese werden durch einen Demultiplexer gefolgt von mehreren Multiplexern (violette Trapeze) zwischen den Nutzern aufgeteilt.

Es existiert in [51] schon ein Testbed von der Deutschen Telekom mit einem verschränkungs-basiertem Multiuser QKD-Netzwerk. Die Topologie folgt der eines Sterns (Photonenquelle in der Mitte) und ist Time-Bin codiert (vgl. Kapitel 7). Demonstriert wurde allerdings bisher nur die gleichzeitige paarweise Schlüsselerzeugung mit vier Nutzern. Damit konnten experimentell bei vier Empfängern mit einzelnen Entfernungen zueinander zwischen 31-77 km SKRs von 25-125 bps erreicht werden. Potentiell können bei vergleichbarer SKR 17 paarweise Nutzer unterstützt werden, theoretisch sollen bis zu 100 Nutzer über insgesamt bis zu 108 km unterstützt werden können [52]. Die verschränkten Photonen werden mittels *Arrayed Waveguide Grating* (AWG) in aktuell bis zu 34 symmetrischen Kanälen (100 GHz Kanalabstand) zwischen den Teilnehmern verteilt. Im realen Testbed [51] wurde ein elektronisch rekonfigurierbarer *Wavelength Selective Switch* eingesetzt, statt dem statischen AWG [52], sowie Clock Recovery.

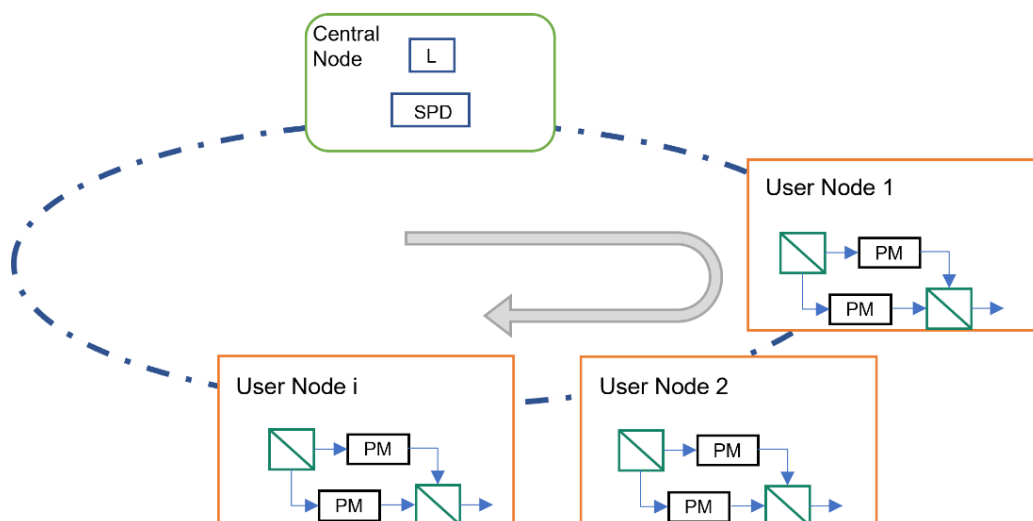
[53] kombiniert experimentell eine polarisationsverschränkte Quelle basierend auf Aluminiumgalliumarsenid mit DWDM Standard-Kommunikationsequipment (OptoLink) über 50 km Faserspule für vier Teilnehmer. Dabei sind die ITU-Kanäle fest zugeordnet: Um den zentralen Kanal 25 liegen symmetrisch je vier Kanäle oberhalb für Bob bzw. unterhalb für Alice. Die Photonenguelle von polarisationsverschränkten Bell-Zuständen kann flexibel angeordnet werden und es besteht keine Notwendigkeit für stabilisierende Interferometer, dafür aber für Polarisationskontrolle und Kühlung. Das Post Processing erfolgt noch nicht in Echtzeit. Auch wenn hier aktuell im passiven Fall jeder Teilnehmer vier SPDs benötigt, kann mit zeitlichem Multiplexing die Anzahl der benötigten SPDs auf eins reduziert werden. Die erreichbaren SKRs liegen allerdings auch im Back-to-Back-Fall bei nur wenigen bps. Dieses erste Experiment mit einem verschränkte-Photonen-generierenden Chip für Standard-Telekommunikationsequipment zeigt, dass noch spezielles Equipment benötigt wird, z.B. SNSPDs zur Erhöhung der Detektionseffizienz, wie auch eine sorgfältige Einkopplung, um höhere SKRs über mittelreichweitige Strecken zu übertragen.

### Weitere Multiuser Protokolle

Es existieren mittlerweile auch erste Ansätze, Protokolle für Multiuser Netzwerke zu erweitern, die bisher noch nicht im Zusammenhang mit Multiuser standen. Allerdings haben sich diese Protokolle noch nicht so etabliert, wie TF und verschränkungs-basierte QKD. Dennoch zeigen diese Entwicklungen, dass viele QKD Protokolle für Multiuser-Topologien erweitert werden können. Wichtig ist aber bei jedem vorgeschlagenen Protokoll, dass es die nötigen Sicherheitsbeweise erfüllt. Es werden exemplarisch Protokolle ausgehend von dem CV-Protokoll (vgl. Kapitel 1) und von DPS vorgestellt, sowie ein auf DV basierendes Protokoll für eine kommerzielle Bus-Topologie.

In [54] wird ein simultanes P2MP-Protokoll basierend auf CV QKD demonstriert, welches ausgehend von demselben kohärenten Zustand des Senders mehreren Empfängern unabhängige Kommunikation ermöglicht. Der Vielphotonenzustand wird durch passiven Splitter (verlustbehaftet) an alle Empfänger verteilt. Bei jedem Nutzer kommt daher ein leicht anderer Zustand an, während aber alle Nutzer zum Sender und untereinander korreliert sind. Je mehr Nutzer im Netzwerk vorliegen, desto höher ist durch die zusätzlichen Messungen die Sicherheitsabschätzung und damit die SKR, aber desto größer sind auch die Verluste durch die Strahlteiler. Bei der Reverse Reconciliation wird nochmals mittels Einmalverschlüsselung für den Versand an den Transmitter verschlüsselt, um das Kombinieren der Informationen von mehreren korrelierten Bobs zu vermeiden. Der aus der Einmalverschlüsselung entstehende Schlüsselverlust kann bei gescheiterter Fehlerkorrektur nicht kompensiert werden. In der Privacy Amplification wird versucht, zwischen Sender und jedem Empfänger einen unabhängigen Schlüssel zu erzeugen, also die Korrelationen zwischen verschiedenen QKD-Verknüpfungen nachträglich zu entfernen. Das theoretische Protokoll kann laut Simulation 128 Nutzer über 125km mit einer SKR von 54 kbps erreichen.

Dagegen präsentiert [55] eine Ringstruktur für ein Protokoll basierend auf DPS QKD. *Abbildung 10* zeigt, dass sich alle Teilnehmer in einer gemeinsamen Verbindungsstrecke befinden, sodass nur in einem Knoten Sender/Empfänger benötigt wird und alle dazwischenliegenden Teilnehmerknoten (~6) über insgesamt 100 km paarweise miteinander kommunizieren können. Dabei wird unterschieden, ob die Schlüsselerzeugung zwischen zwei Nutzerknoten<sup>3</sup> oder zwischen dem zentralen Knoten und einem Nutzerknoten<sup>4</sup> stattfindet. Der vom zentralen Knoten gesendete kohärente Impulszug wird am 1. Nutzerknoten abgeschwächt und die Phase (an beiden<sup>3</sup>) Nutzerknoten moduliert und vom zentralen Knoten wieder detektiert. Basierend auf dem öffentlichen Ergebnis (welcher Time Slot und Detektor) wird bei (beiden) Nutzerknoten dasselbe Rohschlüsselbit entsprechend dem Detektorausschlag/ der relativen Phase erzeugt. Das Reduzieren der Intensität dient der Abhörsicherheit, während die Implementierung auch gegen eine *Trojan Horse Attack* (THA) sicher ist.

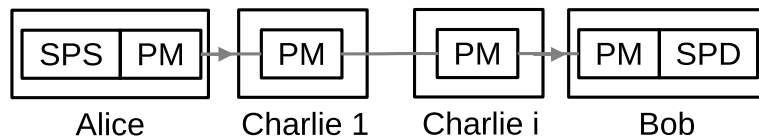


*Abbildung 10: Ringstruktur DPS mit Central Node und mehreren User Nodes [55]. Netzwerk ist einfach um weitere User Nodes erweiterbar. L: Laser, SPD: Single-Photon-Detektor, PM: Phase Modulator, Polarization Beam Splitter.*

<sup>3</sup> Erster Fall

<sup>4</sup> Zweiter Fall

Ähnlich dazu gibt es ein kommerzielles System namens *Qline* von dem französischen Hersteller VeriQloud basierend auf PM DV QKD, bei dem sich die Nutzer ebenfalls hintereinandergeschaltet in einer Linie befinden [56]. Während die technisch aufwendige Erzeugung und Messung der Einzelphotonen-Zustände an den Enden des Bus vorgenommen werden, müssen die Nutzer nur einfache Phasenmodulationen ausführen. Dieses Verfahren wurde bereits in einem Testbed der Deutschen Telekom erprobt und konnte dort über Distanzen bis 40 km bis zu 10 kbps SKR für vier Nutzer bereitstellen [57]. Das Verfahren ist in *Abbildung 11* veranschaulicht.



*Abbildung 11: Qline Architektur [56]. Während alle Nutzer über Phasenmodulatoren (PM) verfügen, benötigen nur Alice und Bob Einzelphotonenquelle (SPS) bzw. Einzelphotonendetektor (SPD) für die Zustandserzeugung und -detektion.*

## Fazit

Um Multipoint-Netzwerke zu realisieren, können verschiedene Techniken eingesetzt werden. Die gängigsten sind die des optischen Splittings/Switchings, wo durch Wellenlängen- oder Zeitmultiplexing Netzwerkverbindungen zwischen beliebigen Nutzern hergestellt werden. Trends in größeren Netzwerken laufen zum dynamischen Switching mittels SDN hin. Es werden aber auch spezielle Multiuser Protokolle aus bereits existierenden Protokollen entwickelt. Dafür eignen sich besonders MDI/TF, da hier das zentrale Relay als Untrusted Node fungiert, oder verschränkungs-basierte Protokolle. Daraus ergeben sich meist Ring- oder Stern-basierte Topologien. Dabei sind je nach Protokoll gleichzeitige Verbindungen zwischen je zwei Teilnehmern möglich oder manchmal sogar eine P2MP-Kommunikation.

Viele kommerzielle Anbieter (Toshiba, IDQ) realisieren bisher den Aufbau von QKD-Netzwerken noch mit paarweisen P2P Verbindungen über Trusted Nodes. Dagegen gibt es aber jetzt schon unterschiedliche kommerzielle Ansätze für echte Multiuser Netzwerke. Dazu zählt Qline von VeriQloud mit reduziertem Hardwareaufwand [56]. Ein zentraler Hub zum Aufbau von Multipoint-zu-Multipoint Netzwerken wurde von Q\*Bird mit WDM-Integration entworfen [58]. Ähnlich dazu eignet sich auch das verschränkungs-basierte QKD-System von Quantum Optics Jena [59] durch seine flexibel positionierbare Photonenquelle und die jeweils lang-/kurzreichweitigen Empfänger für Multiuser Netzwerke. In dem größten europäischen QMAN, MadQCI konnten u.a. die ungekoppelten CV Geräte von Huawei [17] flexibel mit Switches zusammengeschaltet werden.



## 4. Koexistenz mit klassischem Datenverkehr

Obwohl die Sicherheit in Computernetzwerken sehr wichtig ist, ist sie nur in den wenigsten Fällen das oberste Designkriterium und muss sich im Allgemeinen mit anderen Aspekten wie z.B. Performance und Ökonomie arrangieren. Somit muss sich auch die QKD, die nur für den Schlüsselaustausch im Computernetz verantwortlich ist, nach den anderen Anforderungen des Netzwerks richten und nicht umgekehrt. Konkret bedeutet das, dass es vermutlich nur selten explizite Dark Fibers für QKD geben wird und stattdessen die Koexistenz zwischen QKD und klassischem Datenverkehr in der gleichen Netzinfrastruktur ein sehr wichtiger Aspekt ist. Problematisch ist hierbei, dass die Quantensignale nur aus wenigen Photonen bestehen (Leistungen oft nur  $\sim$ pW) und deswegen sehr anfällig gegenüber Störungen durch klassische Signale sind (typische Leistungen  $\sim$ mW). Trotz dieser Herausforderung gibt es bereits jetzt (kommerzielle) Lösungen, die die WDM Kopropagation von QKD und klassischem Tbps Datenverkehr in der gleichen *Standard-Single-Mode-Fiber* (SSMF) erlauben.

### Störungen von QKD durch klassische Signale

Es gibt eine Vielzahl an möglichen Störungen des Quantensignals durch klassischen Datenverkehr [60]. Man unterscheidet, ob die Störungen durch klassische Signale innerhalb des Frequenzbandes des Quantensignals (*in-band*) oder außerhalb (*out-band*) liegen. Letzteres ist insbesondere bei DV QKD relevant, da die verwendeten SPDs nicht wirklich wellenlängenselektiv sind und somit z.B. nach einem Demultiplexer auch die Störphotonen anderer Wellenlängen das SNR des Quantensignals negativ beeinflussen. Abhilfe kann hier beispielsweise durch eine Verbesserung der Kanaltrennung des (De-) Multiplexers, einem erhöhten Wellenlängenabstand oder durch einen engen Bandpassfilter um das Quantensignal vor dem Detektor geschaffen werden.

In-Band gibt es drei wichtige Störquellen [60]:

- *Amplified Spontaneous Emission* (ASE) Störungen: In Verstärkern, wie beispielsweise den häufig verwendeten *Erbium-Doped Fiber Amplifiers* (EDFAs), verursachen Nebenprozesse im aktiven Medium ein breites Rauschen. Dies stellt ein Problem dar, da bei WDM üblicherweise nach dem Multiplexer mit einem EDFA die klassische Signalleistung auf das gewünschte Niveau angehoben wird und somit Störungen auch innerhalb des Frequenzbandes des Quantensignals erzeugt werden. Den ASE Störungen kann allerdings leicht durch Verwendung eines Filters direkt nach dem EDFA begegnet werden.
- *Four Wave Mixing* (FWM) Störungen: In den Glasfasern kann es zu einem nicht-linearen Prozess zwischen den klassischen Signalen kommen, bei dem zwei Photonen vernichtet und anschließend zwei neue Photonen erzeugt werden, die potentiell andere Frequenzen haben und somit auch innerhalb des Frequenzbandes des Quantensignals liegen können. Auch wenn diese Störung normalerweise nicht dominant ist, kann sie beispielsweise durch ausreichendem Frequenzabstand zwischen QKD und klassischem Signal reduziert werden, wie in [61] beschrieben.
- Raman Streuung: Die dominanteste Störung entsteht durch inelastische Raman Streuung der klassischen Signale. Da sie sehr breitbandig ist ( $\sim$ 200 nm), wird ihr üblicherweise durch Reduzierung der *Launch Power* der klassischen Kanäle oder durch Verschieben des QKD Signals in das O-Band begegnet.



### Aktuelle Situation

CV QKD gilt als störungstoleranter, da die kohärente Detektion sehr wellenlängenselektiv ist und außerdem höhere Signalstärken auftreten. Allerdings besitzen DV QKD Systeme derzeit einen Entwicklungsvorsprung. Tabelle 3 gibt einen aktuellen Überblick über realisierte Kopropagation in SSMFs zwischen QKD und klassischem Datenverkehr in verschiedenen Experimenten bzw. Testbeds.

Quelle, CV/DV	Jahr	SKR	Klassische Channels (Traffic), Total Launch Power	Reichweite (Dämpfung)	QKD Wellenlänge
<b>Anmerkungen</b>					
[62], CV	2019	27.2 kbps	100x 24.5Gbaud PM-16QAM (18.3 Tbps), 12.9 dBm	10 km (7 dB)	1550 nm
CV QKD mit Diskreter Modulation, TLO und homodyner Detektion; C-Band Kopropagation mit zusätzlichem Filter nach EDFA; keine Beeinträchtigung durch Kopropagation					
[5], [17], CV	2023	40 bps <sup>5</sup>	5x 10G (50 Gbps), <0 dBm	25.4 km (21 dB)	C-Band (variabel)
CV QKD mit Gaußscher Modulation, LLO und heterodyner Detektion im MadQCI Testbed; C-Band Kopropagation; keine Beeinträchtigungen durch Kopropagation					
[63], CV	2024	>0 bps	8x 200G 16QAM (1.6 Tbps), -1 dBm	25 km	C-Band (variabel)
CV QKD mit Gaußscher Modulation, TLO und heterodyner Detektion; C-Band Kopropagation mit 100 GHz Guard-Band; für Launch Power >-1dBm QKD Beeinträchtigungen (-> 200 GHz Guard-Band)					
[64], DV	2023	100/1 kbps	60x 100G DP-QPSK (6 Tbps), 17 dBm	50 km/70 km (26 dB)	1310 nm
BB84; kommerzielles Gerät von Toshiba; C/O-Band Kopropagation mit zusätzlichem Filter vor SPD; leichte QKD Beeinträchtigungen: 100 kbps vs 170 kbps (@50 km, mit und ohne klassischem Traffic)					
[65], DV	2024	75 bps	8x 100G QPSK (800 Gbps), 10 dBm	100 km	1546.1 nm
BB84; C-Band Kopropagation durch Zeitmultiplex mit Bandpass vor und nach Glasfaser; keine Gegenpropagation möglich!; starke QKD Beeinträchtigungen: 75 bps vs 300 bps (mit/ohne klassischem Traffic)					
[61], DV	2024	1.9/2 kbps	10/65x 100G PDM-QPSK (1/6.5 Tbps), -0.6/-1.9 dBm	100 km	1530 nm
BB84; C-Band Kopropagation durch Abschwächung, Filter nach Glasfaser und top-end SPDs; starke QKD Beeinträchtigung: 15.3 kbps vs 1.9 kbps (klassischer Traffic mit -10 dBm vs -0.6 dBm)					

Tabelle 3: Übersicht zu Kopropagation in SSMFs zwischen QKD und klassischem Datenverkehr

Die oben genannten Beispiele gliedern sich in solche, bei denen die Kopropagation im C-Band oder C/O-Band stattfindet. Bei **C/O-Band Kopropagation** liegt üblicherweise das Quantensignal im O-Band und das klassische Signal im C-Band. Die Übertragung von klassischen Signalen im C-Band bringt zwar den großen Vorteil, dass sie selbst bei normaler Launch Power wenig Störungen im O-Band verursachen und alle klassischen Kanäle genutzt werden können, aber durch die starke Abschwächung im O-Band ist die maximale QKD Distanz auf 50-80 km limitiert. Bei **C-Band Kopropagation** liegen QKD und klassische Signale im C-Band vor, wodurch aufgrund der kleineren Abschwächung von Signalen in Glasfasern in diesem Wellenlängenbereich grundsätzlich größere Reichweiten möglich sind. Bei CV QKD können in diesem Fall die meisten der klassischen Kanäle genutzt werden und es wird nur ein schmales Guard-Band um den QKD Kanal benötigt, der außerdem häufig beliebig gewählt werden kann [17], [63]. Außerdem treten bei geringer Launch Power kaum QKD Performance Einschränkungen auf. Im Gegensatz dazu kommt es im Fall von DV QKD immer zu einer Reduktion von Reichweite und SKR

<sup>5</sup> Finite-Size Effekte nicht (vollständig) berücksichtigt

bei C-Band Kopropagation und es gilt immer die Launch Power der klassischen Kanäle zu minimieren, um die beste QKD Performance zu erhalten. Üblicherweise können außerdem meist nur wenige der klassischen Kanäle verwendet werden. In [65] wird ein WDM und Zeitmultiplexing Schema präsentiert, dass sehr hohe klassische Launch Powers ermöglicht. Allerdings gibt es hier die Bedingung, dass die klassischen Kanäle innerhalb von 200-300 GHz um den Quantenkanal liegen und somit nicht viele klassische Kanäle möglich sind. Außerdem führt auch hier eine Reduzierung der klassischen Launch Power zu einer deutlichen Steigerung der SKR und es ist nur unidirektionale Kopropagation mit den klassischen Daten möglich. Auch wenn dies bei aktuell verlegten SSMF-Paaren mit jeweils unidirektionalem Traffic keine große Einschränkung darstellt, soll hier erwähnt werden, dass es nur bei C/O-Band Kopropagation und CV QKD keine Performance Einschränkungen durch bidirektionalen Traffic gibt.

Zusätzlich muss berücksichtigt werden, dass aktive Netzbauteile wie Netzwerkschwitches, Router aber auch Verstärker das Quantensignal zerstören. Daher bieten sich diese Orte im Netzwerk für Trusted Nodes an oder müssen umgangen werden, beispielsweise mittels *Optical Bypass* [66] oder durch einen passiven optischen Switch wie z.B. bei MadQCI [17].

## Fazit

Obwohl eine Kopropagation mit klassischen Signalen möglich ist, kommt es dabei immer zu einer Reduktion der QKD Reichweite und SKR, da neben Störungen auch immer zusätzliche Verluste durch optische Bauteile hervorgerufen werden. Auch unter Annahme von weiteren Entwicklungen werden somit für lange Glasfaserabschnitte (>150 km) dedizierte Dark Fibers benötigt werden, da dort Störungen und Verluste minimiert werden müssen, um QKD sinnvoll realisieren zu können. Dies spiegelt sich auch bei den aktuellen kommerziellen Geräten der etablierten QKD Hersteller wieder, so haben sowohl Toshiba [67] als auch ID Quantique [68] je eine langreichweitige QKD Geräte-Klasse ohne klassische Kopropagation (beides DV QKD da CV QKD bisher auf kurze Reichweiten beschränkt ist) und eine kurzreichweitige Klasse mit klassischer Kopropagation. Auch das aufkommende langreichweitige TF-Protokoll weist aufgrund der hohen Anforderungen an den Quantenkanal kaum eine Möglichkeit zur Koexistenz auf.

Die Quanten-Kopropagation verschiedener QKD Signale stellt kein Problem dar, somit sollte sich QKD ohne Probleme in ein zukünftiges Quanteninternet zum Austausch generischer Quantenzustände integrieren lassen [17], [69].

## 5. Photonic Integrated Circuits

Bei *Photonic Integrated Circuits* (PIC) handelt es sich um optische Systeme auf Mikrochips mit zwei oder mehr photonischen Komponenten. Sie bilden somit quasi das Optik-Pendant zu integrierten (elektronischen) Schaltkreisen. Die Photonische Integration im Allgemeinen ist sehr vielversprechend, da die Informationsübertragung & -verarbeitung mittels Licht viele Vorteile gegenüber der Kontrolle von Elektronen durch den großen Frequenzbereich von Licht bringt und somit eine erhöhte Bandbreite und Geschwindigkeit der Schaltung ermöglicht. Die photonische Integration von QKD-Komponenten in einen Chip ist deshalb eine weitere vielversprechende Entwicklung, vor allem in Anbetracht der Kommerzialisierung, und wird zukünftig eine einfachere und kostengünstigere Integration von QKD-Systemen in bestehende Telekommunikationsnetzwerke ermöglichen können. Die Kostenreduktion entsteht dadurch, dass die optischen Bauteile, die sonst mit hoher Präzision zusammen gespliced werden müssten, direkt zusammen auf dem photonisch integrierten Schaltkreis platziert werden können. Die photonische Integration in einen Chip verspricht nicht nur QKD-Systeme mit kleinerer/kompakterer Bauweise, sondern auch höhere Leistung bei niedrigerem Energieverbrauch, sowie schnellere Wiederholungsraten. Allerdings ergeben sich aktuell insbesondere bei der Detektion von Einzelphotonen und der präzisen Präparation von Polarisationszuständen auf photonischen Chips immer noch Probleme. Daher lässt sich insbesondere das weit-verbreitete BB84 Protokoll nicht so einfach in PIC umsetzen, weshalb die Integration von gängigen QKD Protokollen meist noch nicht so weit fortgeschritten ist.

### Materialien

Die Forschung und damit die Kommerzialisierung von PIC ist abhängig von der Eignung der jeweiligen Materialien. Für die integrierte Quantenphotonik können unterschiedliche Materialien mit individuellen Vor- und Nachteilen eingesetzt werden: z.B. Silizium, Siliziumdioxid, III-V Verbindungshalbleiter und Lithium Niobat.

Es folgt eine Übersicht über die gängigsten Substrate mit deren jeweiligen Eigenschaften: [2], [70]

#### Silizium

gängige Mikrofabrikationstechniken; Integration mit hoher Dichte in bestehende CMOS-Prozesse möglich	langsame thermo-optische Modulation -> Carrier Injection & Depletion für schnelle Modulation mit phasenabhängigen Verlusten => MEMS-basierte Phasenschieber ohne diese Verluste
--	---

#### Siliziumdioxid

niedrige Propagationsverluste; unkomplizierte Fabrikationstechniken	geringer elektro-optischer Koeffizient -> keine elektro-optische Modulation möglich; langsamere thermo-optische Modulation nötig
---	--

#### III-V Verbindungshalbleiter (z.B. InP, GaAs, AlN)

Schnellste elektro-optische Modulation durch hohe Nichtlinearitäten; Single Photon Emission/ verschränkte Photonen -> geeignet für QKD-Sender; gut verstandene Fabrikationstechniken (mit konventioneller Elektronik); hohe Integrationsdichte möglich	hohe Propagationsverluste
---	---------------------------

## Lithium Niobat

geringe Propagationsverluste; sehr gute Erzeugung (un)verschränkter Photonen; Erhöhung Integrationsdichte -> LNOI (Lithium Niobate-On-Insulator); hohe optische und opto-elektronische Nichtlinearitäten für optische Modulation	schlechte Skalierbarkeit
--	--------------------------

Meist wird nur ein Material verwendet, aber seit 2014 werden auch hybride quantenphotonische Chips mit unterschiedlichen Materialien eingesetzt [70]. LNOI ist ein vielversprechendes hybrides Material [71], denn es ermöglicht zum Beispiel SNSPDs bei kryogenen Temperaturen zur Phasenstabilität einzusetzen und bietet eine bessere Skalierbarkeit im Vergleich zu Lithium Niobat. TriPleX [72], [73], ist eine dielektrische Wellenleiterplattform, die auf alternierenden Siliziumnitrid- und -Siliziumdioxid-Schichten basiert und niedrige Verluste aufweist.

Es wird in der Literatur manchmal zwischen hybrider und heterogener Integration differenziert, wobei der Unterschied in der Fertigung der Verbindung der verschiedenen Materialien besteht. Bei der hybriden Integration werden zwei verschiedene Chips miteinander verbunden (*Packaging*) und bei der heterogenen werden die Materialien direkt auf einem Chip vereint [74]. Dies wird in *Abbildung 12* veranschaulicht.

## Hybride Photonische Chips

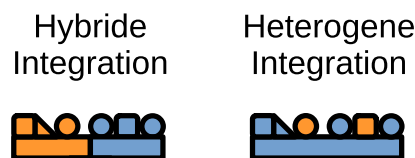


Abbildung 12: Ansätze zur Realisierung hybrider photonischer Chips.

So wird in [75] beispielsweise sowohl Siliziumnitrid (optimal für verlustarme Empfänger) als auch Indiumphosphid (für schnelle *Elektro-Optische Phasenmodulatoren*(EOPMs)) verwendet. Durch die Kombination der Vorteile beider Materialien konnte so eine schnelle Schaltung (1 GHz Wiederholungsrate) mit geringen Ausbreitungsverlusten, sowie daraus resultierender niedriger QBER und hoher SKR von 1.2 Mbps bei 50 km erreicht werden. Die maximal möglichen Reichweiten lagen bei ~250 km. Dabei wird für das asymmetrische MZI Siliziumnitrid eingesetzt und für die EOPMs Indiumphosphid. Würden keine schnellen EPOMs eingesetzt werden, so müssten ausschließlich passive Empfangsstrukturen und somit mehr Detektoren zur Basismessung eingesetzt werden, wie bei den meisten Entwürfen für PICs der Fall ist. Der Grenzflächenverlust zwischen Siliziumnitrid und Indiumphosphid wirkt sich gering mit weniger als 1 dB aus. Die Laser sind allerdings noch nicht auf dem bidirektionalen PIC integriert worden, der gleichzeitig als Sender und als Empfänger fungieren kann.

Häufig wird aber für den gesamten Chip Silizium verwendet, um die geringen Ausbreitungsverluste mit schnellen Geschwindigkeiten zu vereinen. Doch aufgrund des schwachen elektrooptischen Effekts werden bei der Siliziumphotonik zur schnellen Modulation Plasmadispersionseffekte (z.B. *Carrier-Depletion-Modulation* (CDM)) benötigt. Eine vollständig integrierte Lichtquelle für unverschränkte Photonen innerhalb einer Silizium-Photonik-Plattform existierte bis Ende 2024 nicht [76]. Meist wird InP für die Integration des Lasers genutzt [73], [77]. Detektoren hingegen, wie SNSPDs [78] ( $\text{Si}_3\text{N}_4$  Chip), sowie homodyne Detektoren [79] werden bereits häufig in die Silizium-Photonik integriert [2].

## Eignung der verschiedenen QKD-Protokollfamilien für die Chipintegration

Die Integration von **DV QKD** ist bereits recht weit fortgeschritten. Neben dem weitverbreiteten BB84 Protokoll gibt es auch andere QKD-Protokolle, jeweils mit sehr individuellen Anforderungen. Die Herausforderungen bei PIC Systemen mit dem klassischen BB84 Protokoll, wie die Polarisations sensitivität, die Phasenstabilität und die phasenabhängigen Verluste (CDM bei Silizium), sind mittlerweile meist hinreichend überwunden [80], [81], [82]. Nach einer ersten Realisierung eines integrierten QKD-Transmitters mit BB84 [83] im Jahr 2016, wurde im folgenden Jahr ein integrierter Sender (Silizium) und Empfänger ( $\text{SiO}_x\text{N}_y$ ) über eine Strecke von 20 km in [82] entwickelt. Es wurden die grundlegenden Komponenten für eine schnelle Modulation von Quantenzuständen auf Silizium-Photonik geschaffen: die Kombination der langsameren, idealen thermo-optischen Phasenmodulation und der schnellen (10 GHz), aber fehlerreichen (phasenabhängiger Verlust + Sättigung) CDM. Damit können sowohl polarisationscodiertes & Time-Bin-basiertes BB84 als auch das COW-Protokoll bei einer Wiederholungsrate von 1.72 GHz realisiert werden. Zudem verspricht die gute Verfügbarkeit von echten Einzelphotonenquellen auf photonischen Chips eine Leistungssteigerung, da dadurch auf Decoy States verzichtet werden könnte. Insbesondere bei der Realisierung von hohen Reichweiten, stellt die schwierige Integration von SNSPDs auf die photonischen Chips aber ein Problem dar.

**CV QKD** bringt den Vorteil mit, dass dieses Protokoll nicht auf Einzelphotonendetektoren basiert und so der Empfänger potentiell leichter integriert werden kann. Allerdings muss beim Entwurf von CV-Chip-basierten Empfänger-Systemen auf ein sehr geringes und stabiles Detektorrauschen geachtet werden, was insbesondere bei sehr schnellen Detektoren mit großer Bandbreite schwierig ist. Ein wichtiger Parameter hierbei ist die *Clearance*, die die Trennung zwischen dem (zusätzlichen) elektronischen Rauschen und dem (fundamentalen) Schrotrauschen beschreibt [84]. Das in [84] vorgestellte System mit einer Reichweite von 28.6 km und 0.5 GHz Wiederholungsrate verfügt über einen integrierten homodynen Detektor basierend auf LLO und konnte eine SKR von 1.38 Mbps erzielen. In [79] wurden auf einem Silizium-Chip sowohl Sender, als auch Empfänger realisiert. Beim Sender wurde allerdings eine externe Laserquelle verwendet. Das Experiment auf einer 2 m-Faser erzielte eine SKR von 0.25 Mbps. Die homodyne Detektion basierte hier auf einem TLO Schema, wobei das Schrotrauschen des LOs vom restlichen Hintergrundrauschen differenziert werden konnte.

Analog zum nicht-integrierten Fall liegt aktuell ein Entwicklungsrückstand bei der Integration von CV QKD im Vergleich zu DV QKD vor, sodass die Integration weniger vorangeschritten ist. Allerdings gilt CV QKD aufgrund seiner besonderen Eigenschaften als besser geeignet für die photonische Integration, weshalb bereits einige kommerzielle Firmen die Integration von CV QKD als explizites Ziel formuliert haben und sehr aktiv daran forschen.

Auch in dem Bereich der **verschränkungs-basierten QKD** wird PIC eingesetzt, aber meist nur dazu, um verschränkte Photonenpaare zu generieren, was sich häufig sehr leicht auf photonischen Chips realisieren lässt, siehe z.B. [85].

Für **High Dimensional (HD) QKD** (vgl. Kapitel 7) gibt es ebenfalls Ansätze zur Chipintegration. Dabei gestaltet sich die Integration bei gewissen Freiheitsgraden schwieriger als bei anderen: Die Polarisation ist problematisch auf dem Chip zu integrieren, ebenso wie *Orbital Angular Momentum* (OAM). Geeignet sind hingegen Frequenz und Pfad. In [86] wurde beispielsweise eine multidimensionale Verschränkung von Pfad-codierten, hochdimensionalen Zuständen auf einem Chip demonstriert. Dabei wurden 16 identische Photonenquellen auf dem Chip integriert, auf dem neben der Generierung auch die Verarbeitung stattfindet.

Erst kurz vor der Fertigstellung dieses Dokumentes wurde auch der erste Artikel zum integrierten **TF**-Protokoll (vgl. Kapitel 2) publiziert [28], welches sich durch seine benötigte hohe Kohärenz als sehr

schwierig zu integrieren erweist. Mit aktiver Phasenstabilisation auf der Faser können Reichweiten von bis zu 468 km bei 1 GHz Wiederholungsrate erreicht werden.

Oft fehlt es allerdings auch an Sicherheitsbeweisen und -tests vor allem bezüglich der praktischen Umsetzung von QKD auf PICs [87]. Wie [88] zeigt, kann mit richtig entworfenen PIC Systemen sogar die Sicherheit verbessert werden: Durch den Geschwindigkeitsvorteil beim Schalten der Modulatoren in Bezug zur längeren Rücklaufzeit von den Reflektoren, sollen THAs verhindert werden können.

Für eine ausführliche, tabellarische Übersicht über die verschiedenen integrierten QKD Protokolle & Systeme sei dem interessierten Leser [87] empfohlen.

## Hybride Systeme

Der nächste Schritt der vollen Integration des gesamten QKD-Systems steht gegenwärtig häufig noch aus [87]. Es können zwar heutzutage prinzipiell alle nötigen Funktionalitäten einzeln integriert realisiert werden, wobei die Einzelphotonendetektoren aber die größte Herausforderung darstellen. Da sich die optische Integration der QKD-Systeme noch im Entwicklungsstadium befindet, sind meist nur einzelne Systemkomponenten auf dem Chip integriert. Bei den sogenannten hybriden Systemen sind entweder der gesamte Sender/Empfänger oder Teile davon noch nicht auf dem Chip integriert und liegen somit extern vor. Häufig handelt es sich hierbei um den Laser oder die Detektoren. Außerdem kommt die Verarbeitungshardware hinzu. Derzeitig ist das Packaging von integrierten QKD-Systemen in kommerzielle Geräte schwierig. Erste Schritte in Richtung voll-integrierte Systeme werden im Folgenden vorgestellt.

Eine integrierte Sender- & Empfänger- Schaltung mit 2.5 GHz Wiederholungsrate wurde erst 2023 von [80] publiziert. Beim Empfänger handelt es sich um ein spezielles Aluminium Borosilikatglas mit besonders günstigen Eigenschaften. Dazu zählen geringe Ausbreitungsverluste, sowie geringe Doppelbrechung. Über eine SSMF und *Avalanche Photodioden* (SPADs) wird eine Reichweite von 151.5 km erreicht. Mit den eigens hergestellten, gekühlten SNSPDs mit besserer Detektionseffizienz von 80% werden aufgrund der niedrigeren QBER sogar Distanzen von 202 km erreicht. Bei dem implementierten QKD Protokoll handelt es sich um eine Variation des BB84 Protokolls mit drei Zuständen basierend auf einer Time-Bin-Codierung. Für die Kontrolle, Synchronisation und Kommunikation mit dem klassischen Kanal wird ein externes *Field Programmable Gate Array* (FPGA) eingesetzt. Der Laser, die Einzelphotonendetektoren, sowie weitere Verarbeitungselektronik sind außerhalb des PICs angesiedelt. Dabei muss außerdem beachtet werden, dass es sich hier teilweise um Laborbedingungen handelt: es ist eine Kühlung bei SNSPDs und SPADs erforderlich. Eine Temperaturstabilisierung ist zur Steuerung der Doppelbrechung des Hohlleiters und für die Erhaltung der gleichen Polarisierung nötig, sonst kommt es zur Polarisationsfluktuation. Außerdem gestaltet sich das Zeit-/Polarisations-Tracking als schwierig bei niedriger Detektionsrate. Es ist darauf hinzuweisen, dass bei diesem System Optimierungen mit Nicht-Standard-Equipment vorgenommen wurde, wie z.B. die SNSPDs und zusätzliche Dispersionskompensation. Dadurch und durch die geringen Verluste der Chips konnten sehr hohe SKR-Werte erreicht werden (SPAD @ 151.5 km: SKR von 1.3 kbps vs SNSPD @202 km: SKR von 9 kbps).

Toshiba hat in seiner Veröffentlichung von 2023 [77] ein voll-integriertes QKD System vorgestellt. Dabei stellen diese ersten eigenständigen, photonisch integrierten QKD-Systemchips einen dringend benötigten Schritt angesichts der häufigen Integration einzelner Funktionselemente statt der vollständigen Systemintegration dar. Herausforderungen wie die On-Chip-Erzeugung von Quantenzufälligkeit, die Komplexität des Elektronikdesigns, das Packaging, der Echtzeitbetrieb mit Stromverbrauch und das Wärmemanagement wurden daher oft nicht berücksichtigt. Diese Punkte stellen gleichzeitig elementare Designkriterien dar, deren Untersuchung für eine Kommerzialisierung



unerlässlich sind. Auf dem Transmitter Chip (InP) sind zwei *Distributed Feedback Laser* integriert, sowie ein MZI und ein *Electro Absorption Modulator* für die On-Off Modulation. Die Lichtquelle wird direkt über ein *Phase-Seeding* phasenmoduliert. Damit kommt der Chip ohne elektrooptische Phasenmodulatoren aus, was diesen kompakter und energieeffizienter macht. Der Empfänger Chip besteht aus einem asymmetrischen MZI und Verzögerungsleitung. Zur Vermeidung von hohen Rauschverlusten wurde das passive Material SiN verwendet. Ein externer Phasenmodulator, sowie die SPADs sind aber auch hier nicht auf dem Chip integriert. Mit diesem System können auf SSMFs Reichweiten von bis zu 50 km bei SKRs von mindestens 28 kbps bis zu 470 kbps überbrückt werden. Die Wiederholungsrate beträgt 1 GHz. Der integrierte Chip wird in einem 19 Zoll Rack für den Betrieb mit zusätzlicher Verarbeitungshardware verbaut.

In China ist man mit der Entwicklung von QKD-Systemen typischerweise weiter fortgeschritten, so auch bei PIC. [81] stellt eine vielversprechende Demonstration eines BB84-basierten Chips auf Silizium da, der alle Komponenten zur Schlüsselverteilung und Hilfsaufgaben auf einem Chip kombiniert. Das System soll über kommerzielle Strecken Reichweiten von 50 km bis zu 150 km unterstützen. Das fertig gepackte Decoder Chip-Gehäuse besitzt am Ende die Maße 3.95 cm x 2.19 cm x 0.90 cm.

Erste PICs sind schon auf dem Weg zu Kommerzialisierung. Das Feldexperiment aus [89] nutzt beispielsweise fertige Sender- & Empfänger-PICs von der Firma KETS (KETS DV-QKD v0.3). Allerdings sind diese jeweils noch in 19-Zoll Racks (2U) mit anderen, nicht integrierten Komponenten, wie den Photonendetektoren, FPGA sowie weiterer Elektronik und Nachverarbeitungshardware verbaut.

## Fazit

Die integrierten Systeme befinden sich noch sehr stark in der Entwicklung. Allerdings existieren in allen Bereichen und Protokollen Bemühungen, diese auf einem Chip zu integrieren. PIC-basierte QKD-Systeme sind noch sehr experimentell. Viele Systeme sind außerdem nicht vollständig integriert: Laser und Detektoren werden häufig extern angeschlossen, da hierfür meist noch keine geeigneten Materialien zur Verfügung stehen. Eine elektronische Treiberschaltung und weitere Verarbeitungshardware werden aktuell oft separat von der Platine betrieben. Darüber hinaus ist die Feinabstimmung der integrierten Komponenten insbesondere in Bezug auf die Modulatoren mit Temperatur- und Phasenabweichungen, aber auch der Polarisation sehr kritisch und erfordert oft manuelles Tuning unter Laborbedingungen. Derzeit wurde noch kein Feldexperiment als Vorbereitung einer Kommerzialisierung mit voll-integrierten PICs durchgeführt, auch wenn bereits eines mit hybriden Systemkomponenten unternommen wurde. Falls integrierte Schaltungen mit hohen Reichweiten getestet werden (häufig nur simulierte Ergebnisse), werden diese meist nur im Labor mittels Faserspulen erreicht. Bei geeigneter Integration ergeben sich allerdings schnellere QKD-Systeme mit höherer Leistung, niedrigerem Energieverbrauch und Geschwindigkeiten von bis zu 2.5 GHz.

Es sind bisher keine voll-integrierten QKD-Systeme kommerziell zu erwerben. Hersteller, die sich aktiv darauf konzentrieren sind Toshiba, KEEQuant und auch IDQ. Wegen der aktuell noch geringen Nachfrage ist die wirtschaftliche Motivation PIC voranzutreiben bei den Herstellern meist recht klein, da in absehbarer Zeit vermutlich keine entsprechend hohen Stückzahlen erreicht werden. Abhilfe schaffen hier Forschungsprojekte die die Integration vorantreiben. Falls die Integration gelingt, so wird die Erweiterung mit QKD bereits existierender Netzwerke einfacher und billiger als bisher ermöglicht.

## 6. Multi-Core Fiber

*Multi-Core Fibers* (MCFs) bestehen im Gegensatz zu den weitverbreiteten SSMFs aus mehreren Glasfaserkernen im Mantel, teilweise beim selben Manteldurchmesser wie SSMFs, während manche MCFs aber durchaus dicker ausfallen können. Durch diese kompaktere Bauweise versprechen MCFs eine Erhöhung der Kanalkapazität und sind außerdem vielversprechend für die Ermöglichung von Koexistenz von klassischen und Quantensignalen, indem SDM neben dem gängigen WDM ermöglicht wird. MCFs werden daher auch oft im Zusammenhang mit HD QKD eingesetzt. Außerdem ist eine Kombination mit PIC möglich. Anwendung können MCFs u.a. in Datacentern finden, um den hohen Datenraten gerecht zu werden [90]. Durch die Nutzung von Fasern mit höherer Kapazität entstehen bei der Installation Kostenvorteile.

### Klassifizierung

Es gibt verschiedene Arten von MCFs, die sich durch ihren Koppelgrad voneinander unterscheiden. Gekoppelte Fasern haben einen geringeren Abstand zwischen den Mittelpunkten (*Core Pitch*) als die ungekoppelten Fasern (vgl. Tabelle 4). Dieser bewegt sich ungefähr um die 10-30  $\mu\text{m}$  für gekoppelte Fasern, darüber handelt es sich meist um ungekoppelte Fasern [91]. MCFs weisen mindestens einen Manteldurchmesser von 125  $\mu\text{m}$  bei 4-5 Kernen auf (2022 von ITU standardisiert [92]), es gibt aber auch Fasern mit einem höheren Durchmesser bei gleicher Kernanzahl, um einen besseren Gütefaktor zu erreichen [93]. Höchstens sollte der Manteldurchmesser jedoch 230  $\mu\text{m}$  betragen, um gegenüber mechanischen Belastungen stabil zu bleiben [94]. Es wurde eine Vielzahl von unterschiedlichsten MCFs-Designs entworfen, wobei hauptsächlich an *stark-koppelnden* MCFs (SC-MCF) [95] und an *schwach-koppelnden* MCFs (WC-MCF) [96] (welche das geringere Übersprechen aufweisen) geforscht wird. In [96] wurde eine 7-kernige Faser auf *Trench*-basierend (Absenkung des Brechungsindex) und mit hexagonal angeordneten Kernen mittels der gekoppelten Moden für geringes Übersprechen entworfen. Das Übersprechen ist eine stochastische Größe und wird durch temporäre und longitudinale Einflüsse, wie Biegen und Verdrehen beeinflusst [97]. Zudem führen längere Wellenlängen zu einer Erhöhung des Übersprechens [96]. Generell gilt, je größer der Abstand zwischen den Kernen, desto geringer das Übersprechen. Eine weitere Strategie das Übersprechen zu verhindern ist, dass in benachbarten Kernen eine entgegengesetzte Übertragungsrichtung gewählt wird. Zu empfehlen ist bei WC-MCFs ein Übersprechen von etwa -60 dB, während der Core Pitch um die 40  $\mu\text{m}$  betragen sollte [92].




Kerne			
	<b>Schwach-gekoppelt</b>	<b>Stark-gekoppelt</b>	
	<i>Nicht gekoppelt</i>	<i>Zufällig-gekoppelt</i>	<i>Systematisch-gekoppelt</i>
Supermoden	Keine Supermoden	Supermoden können sich nicht stabil ausbreiten	Supermoden können sich stabil ausbreiten
	Keine Modenkopplung untereinander; leichte Kopplung zwischen Kernen	zufällige starke Modenkopplung während der Ausbreitung -> Übersprechen wird durch DSP verhindert	Moden sind ideal orthogonal/ ungekoppelt zueinander -> Übersprechen wird durch DSP verhindert

Tabelle 4: Faserkopplung bei MCFs nach [98]



SC-MCFs gliedern sich in *zufällig-gekoppelte* MCFs (RC-MCFs) und *systematisch-gekoppelte* MCFs mit der stärksten vorliegenden Kopplung [98]. Letztere generieren von der starken Kopplung erzeugte Supermoden (Superposition von Moden der einzelnen Kerne). SC-MCFs erfordern ein extra DSP mit *Multiple-Input-Multiple-Output*, da die orthogonalen Eigenmoden dazu neigen überzusprechen. RC-MCFs weisen eine dazu geringere Kopplung auf, sodass sich keine Supermoden stabil über die gesamte Faser ausbreiten können, sondern es existieren zufällige Bereiche, in denen unabhängig plötzlich starke Kopplungen zwischen Moden während der Ausbreitung auftreten können [98]. Die Vorteile von SC-MCFs bestehen in der Verringerung von Nichtlinearitäten, von Modendispersion und von den daraus resultierenden Verlusten [98], [99]. Häufig finden diese Anwendung in langreichweitigen Systemen. Gerade RC-MCFs eignen sich hierfür besonders, da diese durch ihre abschnittswise Schwankungen in der Modenkopplung in einer geringen Akkumulation von *Differential Group Delay* resultieren.

Die mehrfachen Kerne können auch aus Multimodenfasern (einem weiteren SDM-Verfahren) bestehen, sodass beide Verfahren zu einer Multi-Moden MCF kombiniert werden können. Es können auch nur einige wenige Moden unterstützt werden, wie bei der *few-mode* MCF. Die in [100] untersuchte 36-kernige Faser beinhaltet 3 Moden und drei Typen von Kernen. Auch eine *few-mode Fiber* (FMF) alleine kann im QKD-Umfeld vielversprechend bei höheren Reichweiten eingesetzt werden [101].

Eine weitere Klassifikation von MCFs bezüglich Brechungsindex, Moden, Dispersionsverschiebung und Kernanordnung kann [97] entnommen werden. Trench- & Hole-basierende MCFs sind spezielle Fasern, die das *Inter-Core* Übersprechen minimieren sollen und verfügen deshalb über verschiedene Brechungsindizes im Mantel.

Wichtig bei der technischen Umsetzung von MCFs ist die Kanalisolation zwischen den Kernen. Bei der Übertragung über MCFs stellt das nicht-lineare Rauschen, verursacht durch Raman Scattering, FWM und Inter-Core Übersprechen ein gängiges Problem dar, wobei es sich bei Raman Scattering und FWM noch um die geringsten Störfaktoren unter normalen Bedingungen handelt [102]. Dagegen ist das Übersprechen ein sehr stark limitierender Faktor.

Es gibt im Zusammenhang mit MCFs zwei Arten von Übersprechen [103]:

- *Leakage*: Durch eine evaneszente Feldkopplung über den Mantel hinaus streuen die Photonen gleicher Wellenlänge des Datenlasers in benachbarte Kerne (kann rausgefiltert werden bei unterschiedlicher Wahl von  $\lambda_{\text{QKD}}$  und  $\lambda_{\text{klassisch}}$ ).
- *Raman Crosstalk*: Raman Scattering (erzeugt von den starken klassischen Signalen) streut in Nachbarkanäle der Faser (abhängig von Kanalleistung).

### Einsatz MCFs mit QKD

Das erste Testbed mit MCFs basierend auf einem MCFs-Testbed in L'Aquila in Italien (2019) [104] wurde 2023 nun auch mit QKD Signalen getestet [105]. Das Testbed verfügt generell über ein Kabel mit drei verschiedenen Arten von MCFs: 4-kernige RC-MCFs (C- & L-Band) und WC-MCFs (O- & L-Band), sowie 8-kernige WC-MCFs (O-Band). Eingesetzt für die Nutzung von HD QKD (siehe Kapitel 7) wurde ein 2x26 km langes Kabel mit 4 Kernen (ungekoppelt -> vernachlässigbares Übersprechen < - 40 dB), woraus sich eine SKR von 51.5 kbps ergibt. Hier werden die Kerne für eine 4-dimensionale Übertragung in Zeit und Pfad genutzt. MCFs eignen sich besonders hierfür wegen ihres niedrigen Phasendriffs. Die relative Phase zwischen den Kernen spielt eine wichtige Rolle und muss bei zu hohem Phasendrift z.B. durch OPLLs stabilisiert werden. Die niedrigen SKRs resultieren daraus, dass bei mehrdimensionaler

QKD mehrere Detektoren eingesetzt werden, die aber vermehrt *Dark Counts* aufweisen, sodass das SNR sinkt. In vergleichbaren Veröffentlichungen werden ähnliche SKRs erreicht [106].

2016 zeigte [103] als erstes Experiment, dass QKD-Signale mit klassischen Daten mit voller Launch Power in MCFs koexistieren können, allerdings war der Quantenkern festgelegt auf eine bestimmte Position. Deshalb soll in [102] die Belegung der verschiedenen Kerne flexibel - ähnlich wie die Wellenlängen - zugeordnet werden, da das Übersprechen auch immer abhängig von der Kernbelegung und der Distanz der Kerne ist. Es werden mehrere *Routing-Core-Wavelength-Resource-Allocation* Algorithmen vorgestellt, die unterschiedliche Ziele verfolgen sollen. Ein Algorithmus ist speziell auf die Wahrnehmung des Übersprechens ausgerichtet, um die Route und die Kerne des Quantenkanals dahingehend auszuwählen, dass das Quantensignal möglichst ungestört verbleibt. Ein weiterer ist darauf ausgelegt, das Spektrum voll auszunutzen, indem vorher die benötigte Verteilung berechnet wird. Ergänzend werden noch zwei weniger rechen- und zeitintensivere Algorithmen verwendet. Der einfachste berücksichtigt nur die Routingzuweisung, und wählt die Allokation von Kern und Wellenlänge zufällig, während der andere zusätzlich die Zuordnung der Kerne festlegt.

Ein anderes Testbed [107] von 2023 nutzt die Koexistenz-Eigenschaften von CV QKD-Signalen mit klassischen Signalen über MCFs aus. So wird über ~17 km durch eine 7-Kernfaser 35 Mbps SKR und 22.8 Tbps an klassischen Daten (89 Kanäle) pro Kern ermöglicht, wobei das CV QKD-Signal zusammen mit den klassischen Daten über die Faser auf unterschiedlichen Wellenlängen im C-Band übertragen wird. Bei ausreichend großem Kanalabstand (>1.8 nm) und je kleiner die Launch Power (<3.5 mW), desto größer ist die SKR.

Vergleichbar dazu wird bei der Koexistenz mit DV QKD in [108] die beliebige Belegung der Kanäle mit einem Quanten- und mehreren klassischen Signalen bei 73 bps SKR / 11.2 Tbps (Koexistenz im zentralen Kern; Launch Power = -9.5 dBm) über eine 7-Kern-Faser von 1 km Länge untersucht. Dabei wird das QKD-Signal zur Reduktion des Ramanrauschens gefiltert, wozu ein minimaler Quantenkanalabstand von 17 nm ermittelt wurde, unter dem keine QKD-Schlüsselgenerierung mehr möglich ist. Wird die optische Launch Power angehoben, steigt die QBER und die SKR sinkt. Sobald die Launch Power über einen maximalen Wert (hier: -9.5 dBm) angehoben wird, führt dies zu Raman Crosstalk, welcher eine QKD-Übertragung in benachbarten Kanälen unmöglich macht. Dagegen kann bei Verzicht auf klassische Kanäle im zentralen Kern bei einer Launch Power von +5dBm und insgesamt 9.8 Tbps klassischen Daten, die höchste SKR von 1.2 kbps erreicht werden. Ab der Kombination mit einem dritten klassischen Kanal sinkt die SKR deutlich ab [108], [109].

Die SKR wird stark beeinflusst, wenn klassische Daten im selben Kern übertragen werden (vgl. Kapitel 4), weshalb zu empfehlen ist, einen eigenen Kern für die QKD-Übertragung zu reservieren [110]. Somit bieten sich MCFs für die QKD-Übertragung mit klassischen Signalen an.

## Fazit

Generell werden je nach Störung durch klassische Kanäle typischerweise einige kbps an SKRs für DV QKD in Kombination mit klassischen Daten in einer SSMF erreicht. Die maximale SKR für DV QKD einer heterogenen MCF mit 37-kernigen Faser (7.9 km) dagegen betrug 2019 2.86 Mbps pro Kern (insgesamt 105.7 Mbps) mit 370 Gbps an klassischen Daten [111]. Eine Übersicht der Koexistenz via MCFs von 2022 ist [112] zu entnehmen. Allerdings sind die Teststrecken meist nur wenige km lang, da für höhere Reichweiten die Launch Power der klassischen Signale erhöht werden müsste, was wiederum die QKD-Signale noch mehr beeinträchtigen würde.

Trotz der vielversprechenden Erhöhung der Kanalkapazität und der Koexistenzeigenschaften durch räumliche Isolation der MCFs, gibt es noch weitere Möglichkeiten diese durch den Einsatz anderer spezieller Fasern zu vergrößern. Zeigt [101], den Einsatz einer FMF mit nur einem Kern. Es konnten

hohe Datenraten (100 Gbps klassische Daten/ 1.3 kbps SKR) bei einer Länge von 86 km durch die Vorteile der Modenisolation und der hohen effektiven Fläche einer FMF erreicht werden. Eine erst kürzlich erschienene Veröffentlichung [113] verspricht hingegen mit einer speziellen Methode zur Rauschunterdrückung und Wellenlängenallokation höhere Reichweiten bei der Koexistenz von QKD- und klassischen Signalen von 165 km über MCFs als über die auch untersuchten *Hollow-Core* Fasern zu erreichen. Werden allerdings die beiden Signale jeweils im O- und im C- Band getrennt voneinander betrieben, so sollen MCFs den *Hollow-Core* Fasern in der Leistung des QKD-Signals unterlegen sein, weil das Rauschen auf QKD-Signalen besser reduziert werden konnte.

Folglich besteht auch weiterhin Raum für Verbesserungen an neuen MCFs, sowie dazugehörigen Signalverarbeitungs-Algorithmen, Datenmodulationsschemata, Empfängerkomplexität, sowie die Verbindung der Kerne an den Faserenden. Verglichen mit den erreichbaren Werten aus Kapitel 4, stellt man fest, dass MCFs zwar manchmal hohe Kapazitäten aber oft nur sehr kurze Reichweiten erreichen und so noch kein herausragender Vorteil auf längeren Strecken im Vergleich zur QKD-Übertragung in einer SSMF ersichtlich ist. Zudem scheint das Forschungsgeschehen seit Jahren breit in alle Richtungen gelaufen zu sein, sodass eine allgemeine Standardisierung benötigt wurde, um eine Senkung der Produktionskosten zu beschleunigen. Derzeit scheint kommerzielles Interesse für MCFs in optischen Kommunikationsnetzen hauptsächlich im Bereich der Intra-Datencenter-Kommunikation zu bestehen. Darüber hinaus bieten sich spezielle *Fiber Bragg Gitter*-basierte *Spun*-MCFs als 3D-Sensor an. Durch die Verdrillung der Kerne können Abweichungen in der Belastung oder sogar der Temperatur erfasst werden, sodass diese in der Medizin als Bewegungssensoren und sogar zur Formrekonstruktion in der Endoskopie eingesetzt werden [114].

## 7. High-Dimensional QKD

Um den sich zunehmend erhöhenden Datenraten auch im QKD-Umfeld gerecht zu werden, müssen Verfahren zur Erhöhung der Kapazität im gleichen Maße ausgebaut werden. Eine vielversprechende Möglichkeit hierfür ist die Nutzung mehrdimensionaler Freiheitsgrade (engl. *Degrees of Freedom* (DoFs)) der Photonen. Während gängige DV QKD Protokolle, wie z.B. BB84 auf QuBits (zweidimensionaler  $d = 2$  Zustandsraum (auch Hilbertraum)) basieren, werden bei der HD QKD QuDits ( $d > 2$ ) genutzt, die mehrere Zustände pro Photon kodieren können. Bei QuBits liegen also pro Basiswahl zwei mögliche Messergebnisse vor, während bei QuDits eine entsprechend höhere Anzahl an möglichen Messergebnissen ( $> 2$ ) vorliegt.

Es sei hier angemerkt, dass bei der in Kapitel 1 beschriebenen CV QKD kontinuierliche Größen mit einem kontinuierlichen, d.h. unendlich-dimensionalen Zustandsraum vorliegen. Daher handelt es sich bei CV QKD strenggenommen auch um HD QKD. Der Fokus dieses Kapitels liegt allerdings auf diskreten Systemen mit endlichem Zustandsraum.

Durch die Verwendung von hoch-dimensionalen Zuständen erhöht sich automatisch die Informationskapazität des Kanals, da pro Photon  $\log_2 d$  klassische Bits übertragen werden, wodurch sich die Anzahl der benötigten Photonen zur Übertragung von Informationen reduziert und somit außerdem eine Übersättigung des Detektors vermieden werden kann [2]. Außerdem sinkt der Effekt des Kanalrauschens auf das QKD Protokoll [115], da höher-dimensionale Zustände resistenter gegen Abhören sind, und hoch-dimensionale Verschränkungen stabiler sind. Da sich aufgrund des reduzierten Effekts des Kanalrauschens die maximal tolerierbare QBER erhöht und durch die stabileren Verschränkungen die QBER zusätzlich reduziert wird, erhöht sich zusammen mit der vergrößerten Informationskapazität automatisch die maximal mögliche SKR.

Allerdings werden für die Detektion hochdimensionaler Zustände, bei der die QuDits auf die  $d$  orthogonalen Basiszustände der gegenseitig unverzerrten Basen projiziert werden, mehr Detektoren bzw. mehr Detektionszeit benötigt. Dies führt zu einer erhöhten Sensitivität bezüglich Detektorrauschen, was die maximal erreichbaren Reichweiten reduziert und die Komplexität der Systeme erhöht [105], [115]. Die Reduzierung der benötigten Empfangsstrukturen ist daher ein wichtiger Schwerpunkt der aktuellen Forschung. Analog zu DV QKD benötigt HD QKD leistungsstarke SPDs und Einzelphotonenquellen bzw. abgeschwächte Laserpulse mit Decoy States zur Vermeidung von Seitenkanalangriffen. Da die Gesamtinformationsdichte pro Dimension mit  $\frac{\log_2(d)}{d}$  abnimmt, stellt sich außerdem bei hohen Dimensionen ein Sättigungseffekt ein, sodass das aufwändige Präparieren von hochdimensionalen Zuständen einen zunehmend geringeren Informationsgewinn erzeugt.

Auch wenn die Übertragung der hoch-dimensionalen Quantenzustände grundsätzlich über Freiraum oder Faser (Standard, Multi-Mode oder Multi-Core) realisiert werden kann, müssen z.T. besondere Anforderungen berücksichtigt werden.

### Kategorien

Es können verschiedene Freiheitsgrade der Photonen genutzt werden, um ein hoch-dimensionales Signal durch Erweiterung des Hilbert-Raumes zu erzeugen. Die gängigsten Freiheitsgrade, die einzeln ausgenutzt werden, sind im Folgenden erläutert. Die Vor- und Nachteile der vorgestellten DoFs werden in einer abschließenden Tabelle 5 zusammengefasst. Eine Übersicht über implementierte HD-Protokolle der verschiedenen DoFs mit vergleichenden Parametern findet sich in *Tabelle 6* am Ende dieses Kapitels.

Zeit

Eine einfache Möglichkeit zur Erzeugung hochdimensionaler Zustände ist die Verwendung von Zeit als Freiheitsgrad. Beim häufig verwendeten *Time-Bin* Verfahren wird eine sich wiederholende Folge von diskreten Zeitabschnitten angenommen, deren Anzahl der Dimension  $d$  entspricht [115]. Beispielsweise wird in [116] eine 4-dimensionale Time-Bin Codierung realisiert, bei der in der  $\mathcal{Z}$ -Basis die Information mittels einzelner Time-Bins encodiert werden. Die  $\mathcal{X}$ -Basis hingegen besteht aus einer (phasenmodulierten) Superposition mehrerer Time-Bins, die nur zum Überprüfen der in der  $\mathcal{Z}$ -Basis gewonnenen Bits dient. Dabei ist die gesamte Framedauer an die Totzeit des Detektors angepasst. Die Pulsdauer ist eine entscheidende Größe, da sie ausreichend hoch für den Detektor gewählt werden, aber nicht zu hoch wegen Delays. Der Empfänger misst zufällig (90/10) entweder die Zeit oder die Phase. Für die zeitliche Detektionseffizienz muss hier idealerweise mittels eines Kopplers zwischen vier SPDs umgeschaltet werden. Für die Messung in der  $\mathcal{X}$ -Basis wird die konstruktive Interferenz des zentralen dritten Time-Bins – abhängig vom genommenen Weg der Photonen in drei kaskadierten Interferometern – mittels vier weiterer SPDs ermittelt. Dieser Aufbau benötigt also insgesamt bis zu acht SPDs. Eine kompaktere Empfängerstruktur wird dagegen in [117] geschaffen, die lediglich aus zwei SPDs besteht. Man benutzt hier für die zeitliche Codierung eines Zustands die Kombination zweier Time-Bins innerhalb eines Frames aus vier Time-Bins. In der  $\mathcal{Z}$ -Basis folgen dabei beide Bins direkt aufeinander, entweder in der ersten Hälfte des Frames oder in der zweiten (siehe *Abbildung 13*), sodass nur ein Interferometer mit Delay = 1 benötigt wird. In der  $\mathcal{X}$ -Basis wird dagegen ein Interferometer mit Delay = 2 eingesetzt. Verschachtelt man die Interferometer entsprechend, so kann die Anzahl der SPDs auf zwei reduziert werden. Aktuell gibt es außerdem auch erste Systeme [118], deren Empfängeranzahl (2) wesentlich geringer als die Dimensionalität der QuBits ( $d=8/16$ ) ist und auf einer Time-Bin basierten Puls-Positionsmodulation beruht. [119] demonstriert den Einsatz dieses Systems im Rahmen eines ersten Field Trials. Ein Vergleich der Parameter der verschiedenen Systeme findet sich in *Tabelle 6*.

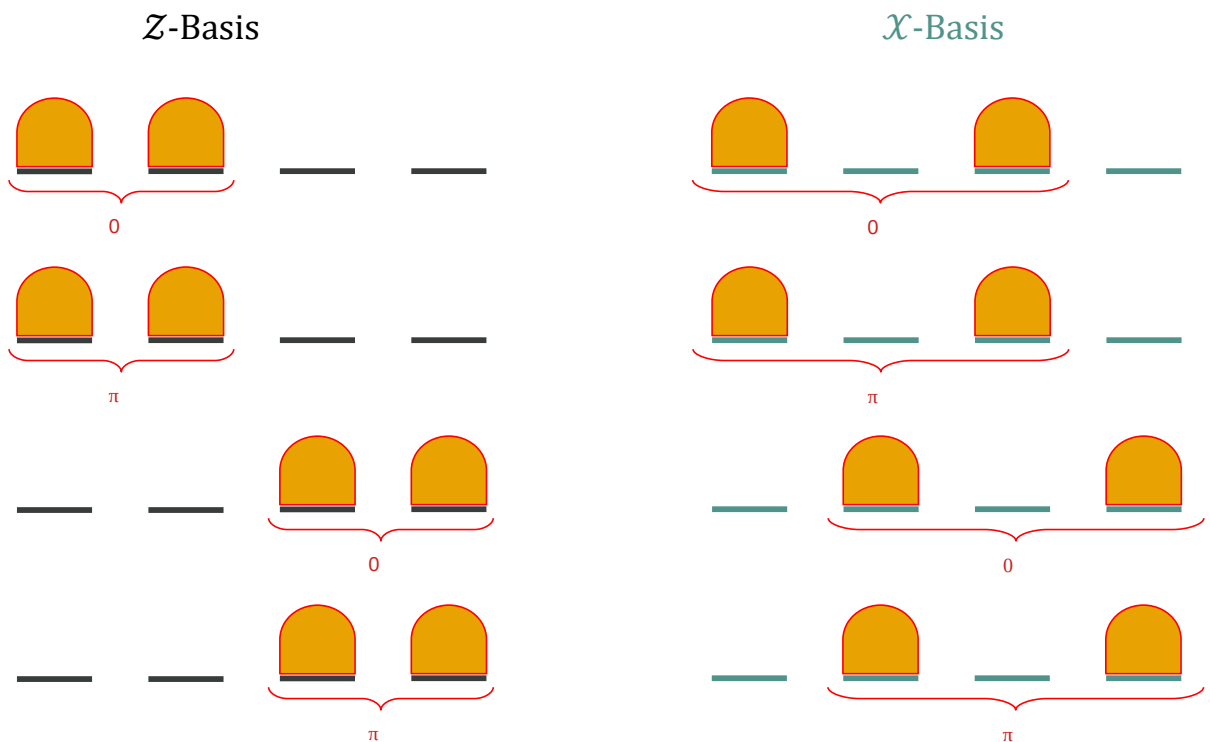


Abbildung 13: **4D Time-Bin Codierung** [117]. In der  $\mathcal{Z}$ -Basis wird die jeweilige Information encodiert, während die  $\mathcal{X}$ -Basis nur zum Überprüfen dient. In Rot wird jeweils die Phasenlage der Pulse zueinander gekennzeichnet.

Ein verwandtes Verfahren ist als *Time-Energy* bekannt, wo durch SPDC innerhalb der in *Time-Bins* diskretisierten Kohärenzzeit des Pumpimpulses zeitverschränkte Photonenpaare erzeugt werden [115]. Eine auch in *Tabelle 6* enthaltene experimentelle Realisierung des Time-Energy-Verfahrens ( $d=3$ ) [120] zeigt, wie stabil diese Verschränkung ist und welche Reichweitenvorteile sich daraus ergeben.

Zeitbasierte Codierungen bringen den Vorteil mit sich, dass sie auf jeder SSMF anwendbar sind und im Freiraum kaum beeinflusst werden. Außerdem können sie einfach mit Standardequipment umgesetzt werden. Es liegen vollständige Sicherheitsbeweise, manchmal ausgehend von CV QKD vor [2]. Es sind hohe Wiederholungsraten [2] und eine einfache Integration mit PIC [115] möglich. Zudem gibt es mittlerweile kompakte Empfängerstrukturen mit wenigen SPDs [117]. Time-Bin basierte Verfahren gehören zu den am weitesten entwickelten im Bereich der HD QKD.

Der Nachteil von zeitbasierten Codierungen liegt in der Verringerung der eigentlichen Symbolrate bei Erhöhung der Dimensionen und fester Wiederholungsrate am Sender [115]. Liegt also beispielsweise ein Sender vor, der mit einer Wiederholungsrate von 1 GHz Time-Bins erzeugt, so resultiert für  $d=2$  eine Symbolrate von nur 500 MHz (da immer zwei Time-Bins für einen Zustand benötigt werden), wenngleich die Informationskapazität durch die Verwendung des höher dimensionalen Zustands erhöht wurde.

## Pfad

Eine weitere Möglichkeit der Realisierung hoch-dimensionaler Zustände ist die Pfad-Encodierung bei der verschiedene Pfadoptionen überlagert werden.

So werden in [121] beispielsweise die Informationen mittels Superposition zwischen zwei Pfaden codiert. Dazu werden die erzeugten Pulse mittels Strahlteiler für die verschiedenen Faserkerne einer MCF aufgetrennt. Dabei übermittelt ein erstes Signal den Zustand, ein unabhängiges zweites Signal, senkrecht polarisiert dazu, dient als Referenz zur gegenseitigen Phasenstabilisierung zwischen den zwei Kernen. Nach der Übertragung über die Faser findet eine Zusammenführung der zusammengehörigen zwei Kerne durch einen weiteren Strahlteiler statt. Am Empfänger werden zusätzlich die Laufzeitunterschiede, die durch die leicht unterschiedlichen Längen der Kerne der MCFs, die Ein-/Auskopplungsgeräte und den Phasenschieber entstehen, durch das Referenzsignal ausgeglichen.

Zur Verbesserung der Skalierbarkeit bietet sich daher insbesondere die Integration mit PIC [86] und die Verwendung von mehrkernigen Fasern für eine getrennte Übertragung mittels einer Pfadkodierung an (vgl. Kapitel 5 und 3). Besonders sollen MCFs die Fragilität der Zustände minimieren, geringeren Phasendrift zwischen Kernen als unabhängige SSMF aufweisen und zudem die Rate nicht negativ beeinflussen [105].

Meist können aufgrund der Phaseninstabilität allerdings nur kurze Strecken realisiert werden. Auch wenn in [86] die Erzeugung und Übertragung eines  $d = 15$  Zustandes demonstriert wurde, stellt die Realisierung hoher Dimensionen insbesondere ohne die gute Skalierbarkeit durch PIC ein Problem dar.

[121] zeigt beispielsweise ein 4-dimensionales System über eine 2 km lange, 7-kernige MCF mit zusätzlicher Phasenstabilisation, um in einer Echtzeit-Implementierung eine SKR von 6.3 Mbps zu demonstrieren. In [55] wird ein Schlüsselaustausch über insgesamt 52 km durch Verwendung einer aktiven Phasenstabilisierung mit einer 4-kernigen MCF durch ein 4-dimensionales hybrides Schema mit zwei Pfaden erzielt.

### Orbitales Drehmoment

Bei dem auch als *Spatial (Mode) Encoding* bekannten Schema werden spezielle Photonenzustände mit orbitalem Drehmoment verwendet. Dabei handelt es sich um eine Quanteneigenschaft der Photonen, die einem Drehimpuls ähnelt. Oft werden *Laguerre-Gauß* (LG) Moden verwendet [122], da diese weniger empfindlich gegen Übersprechen sind [2]. Die Zustände können leicht mit Wellenfrontformender Geräte, wie speziellen Beugungsgittern (generiert mit *Spatial Light Modulatoren*) oder flüssigkristall-basierten *q-Plates*, erzeugt werden, es ist aber auch möglich mittels SPDC direkt verschränkte hoch-dimensionale Photonenpaare zu erzeugen. Es können damit leicht Zustände hoher Dimension realisiert werden und es liegen vollständige Sicherheitsbeweise für daraus bestehende QKD Protokolle, ausgehend von dem Qubit Fall vor. Während sich OAM gut für die Freiraumübertragung eignet, gibt es oft Probleme bei Glasfaserübertragung wegen der mangelnden Phasenstabilität und der Modendispersion [115]. So muss in [123]/[124] eine spezielle Air-Core Multimode-Faser verwendet werden, um die QuDit-Zustände zuverlässig 1.2 km weit mit einer Schlüsselrate von 38 kbps zu übertragen. Außerdem ist die Integration mit PIC sehr kompliziert [121], wenn auch nicht unmöglich [125].

### Frequenz

Es ist auch möglich, hochdimensionale Zustände durch die Superposition verschiedener Frequenzen zu erzeugen. Dies kann beispielsweise direkt bei der Erzeugung verschränkter Photonenpaare mittels SPDC realisiert werden, wie in [126] demonstriert. Allerdings findet hier häufig eine Integration in PICs statt, so wurde beispielweise in [127] bereits die Erzeugung verschränkter, 10-dimensionaler Photonenpaare über 24.2 km demonstriert. Der Vorteil bei der Operation im Frequenzbereich ist, dass die Filter auf mehreren Moden gleichzeitig mittels programmierbarer Phasenfilter und elektrooptischer Modulatoren angewendet werden können, woraus sich eine gute Skalierbarkeit ergibt [127]. Auch wenn diese Methode neben der guten Integrierbarkeit in PICs über eine hohe Kompatibilität mit SSMF und Standardequipment verfügt, weist sie aktuell einen Entwicklungs- und Forschungsrückstand auf. Häufig wird nur die Verteilung von Zuständen aber kein funktionierendes QKD-Protokoll demonstriert.

	Time-Bin	Pfad	OAM	Frequenz
Vorteile	Einfache Encodierung mit wenigen SPDs; hohe Wiederholungs-raten; kompatibel zu SSMF; PIC möglich; vollständige Sicherheitsbeweise -> am weitesten entwickelt	Konzeptionell einfache Encodierung; gute Skalierung durch PIC	Leichte Zustandspräparation hoch-dimensionaler Zustände; vollständige Sicherheitsbeweise; gut geeignet für Free-Space	Gute Integrierbarkeit mit PIC; gute Skalierbarkeit durch vereinfachte Operation im Frequenzbereich; hohe Dimensionen möglich
Nachteile	Erhöhung der Dimensionen verringert Symbolrate bei fester Wiederholungsrate am Sender	Hohe Phasensensitivität bei Übertragung (oft MCF und/oder Phasenkorrektur nötig -> geringe Distanzen); schlechte Skalierbarkeit ohne PIC	Probleme bei der Faserübertragung durch mangelnde Phasenstabilität & Modendispersion; Schwierige Chipintegration	Forschungsrückstand

Tabelle 5: Vergleich DoFs für HD QKD



## Hybride Verfahren

Es ist außerdem oft möglich, die verschiedenen Freiheitsgrade untereinander zu kombinieren um die Dimensionalität weiter zu erhöhen. Auch hier verspricht die Integration mit PIC eine Verbesserung der Skalierbarkeit, auch wenn einige der Freiheitsgrade, wie beispielsweise die Polarisation, nicht immer unbedingt einfach realisiert werden können.

Das schon im Kapitel 6 erwähnte Testbed in L'Aquila nutzt beispielsweise die Kombination aus Time-Path [105]: Dabei handelt es sich um eine 4-dimensionale hybride Time-Path Encodierung über eine 4-kernige Faser deren Länge mit Schleifenbildung 52 km beträgt. Die Zustände werden durch Verwendung eines Strahlteilers und nachfolgender Intensitäts- und Phasenmodulation der Impulszüge auf zwei Pfaden erzeugt und dann über zwei Faserkerne übertragen. Bei der Detektion kann durch die Verwendung von Strahlteilern und insgesamt vier SPDs die Messung in den verschiedenen Basiszuständen realisiert werden.

Es gibt noch viele weitere hybride Verfahren, wie z.B.: Path-Polarization [128], Polarization-Time [129] und Time-Frequency [130].

Es werden allerdings auch Kombinationen von mehreren hybriden Verfahren mit unterschiedlichen Dimensionen untersucht. So wird in [131] ein experimentelles 8-dimensionales QKD-Schema basierend auf Time-Bins, Polarisation und OAM präsentiert, bei dem der  $8d$  Sender auch mit  $4d$  bzw.  $2d$  Empfängern kommunizieren kann. Durch die unabhängige En-/Decodierung der unterschiedlichen DoFs, wird die Kommunikation in einem QKD-Netzwerk mit verschiedenen DoFs an den Terminals ermöglicht. Das „Downsampling“ des Transmitters für einen Empfänger, falls dieser nicht alle DoFs unterstützt, kann dabei ohne einen Hardwareaustausch umgesetzt werden. Somit könnten in einem HD-Quantennetz anstelle von zentralen Netzwerkknoten mit verschiedenen QKD Modulen einfach konfigurierbare HD QKD Module verwendet werden, die je nach Kommunikationspartner andere Protokolle unterstützen. Das verwendete verallgemeinerte BB84 Protokoll mit Decoy States ermöglichte bei nur 10 MHz Wiederholungsrate SKRs von 24.76 kbps bei  $8d$  und 10 dB Kanalverlust bzw. 217 kbps bei  $2d$  und 2 dB Kanalverlust.

Quelle	DoF	# Dimensionen	(Asymptotische) SKR	Reichweite	Wiederholungsfrequenz
[116]	Time-Bin	4	26.2 Mbps	90 km	2.5 GHz
[117]	Time-Bin	4	0.42 kbps 37 kbps	145 km 25 km	297.5 MHz
[118]	Time-Bin	16 8	210 kbps 155 kbps	25 km 131 km	10 MHz
[119]	Time-Bin (Field Trial)	bis 16	183.3 kbps	~4 km	10 MHz
[120]	Verschränkte Time-Energy	3	0.22 bps	242 km	10-20 kHz
[105]	Time-Bin & Pfad (Testbed)	4 (4-core MCF)	51.5 kbps	52 km	487 MHz
[121]	Path	4 (7-core MCF)	6.3 Mbps	2 km	595 MHz
[123]	OAM	4 2	37.85 kbps 22.81 kbps	1.2 km	600 MHz
[127]	Verschränkte Frequenz	10	-	24.2 km	-

Tabelle 6: Übersicht Parameter HD QKD Systeme



## Fazit

Wie dieses Kapitel zeigt, ist es bereits gelungen, die vielversprechenden Eigenschaften von HD QKD, wie die signifikante Erhöhung der SKR auf kurzen Distanzen und die höhere Störungsresistenz, zu demonstrieren. Zur Erzeugung von QuDits werden verschiedene einzelne DoFs der Photonen ausgenutzt, wie Zeit, Pfad, OAM und Frequenz, sowie vielfältige hybride Kombinationen. Es hat sich bisher kein "Standardprotokoll" etabliert, auch wenn Time-Bin Verfahren aktuell am vielversprechendsten wegen ihrer einfachen Implementierung erscheinen. Das Feld der HD QKD existiert dennoch erst seit Mitte der 2000er und ist deswegen weniger weit entwickelt als z.B. klassische DV QKD basierend auf BB84, was sich negativ auf realisierbare Reichweiten und SKRs auswirkt. Bisher gibt es daher auch nur wenige Field Trials, da sich meistens nur theoretisch oder experimentell in *Proof of Concept* Experimenten über kurze Strecken mit den Protokollen befasst wird. Teilweise werden dabei auch nur ausgewählte Zustände der Protokolle präpariert (z.B. [117]). Eine wichtige Ausnahme dazu stellt das Testbed von L'Aquila [105] dar, wo unter Beteiligung des kommerziellen QKD Herstellers QTI vielversprechende Experimente in realistischen Umgebungen durchgeführt wurden. Die zukünftige Entwicklung von HD QKD wird sowohl stark mit den Entwicklungen bei PIC, als auch bei Glasfasern im Zusammenhang stehen, da die Übertragung von HD-Zuständen z.T. besondere Anforderungen an die Integration bzw. die Glasfasern (z.B. MCFs bei Pfad, Air-core bei OAM) stellt. Außerdem könnte eine Interoperabilität zwischen verschiedenen HD QKD Technologien auf dem Quantenlevel ermöglicht werden, wie in [131] untersucht.

## Zusammenfassung

Das Dokument hat einen Überblick über den derzeitigen Entwicklungsstand im QKD-Bereich verschafft:

- **Continuous-Variable QKD & Twin-Field QKD** als neue Protokolle für robustere bzw. langreichweitigere Verbindungen
- **Multipoint QKD** für die vereinfachte Realisierung von Quantennetzwerken mit mehreren Teilnehmern
- **Koexistenz** von Quantensignalen mit klassischem Datenverkehr
- **Photonische Integration** von QKD für die zunehmende Kommerzialisierung
- **Multi-Core Glasfasern** für verbesserte Übertragungsmöglichkeiten von Quantensignalen
- **High-Dimensional QKD** zur Erhöhung der Datenraten.

Für jeden dieser Bereiche wurde der derzeitige Stand der Forschung zusammengefasst, und geschildert, was sich in Kürze wohl für einen kommerziellen Einsatz eignen wird und wo noch Schwächen, aber auch vielversprechende Stärken liegen. Es bleibt abzuwarten, welche Technologien sich auf dem Markt in Zukunft durchsetzen werden.

## Tabellen- & Abbildungsverzeichnis

Tabelle 1: Übersicht zu aktuellen CV QKD Experimenten und Testbeds .....	8
Tabelle 2: Übersicht zu aktuellen TF QKD Experimenten und Testbeds .....	13
Tabelle 3: Übersicht zu Kopropagation in SSMFs zwischen QKD und klassischem Datenverkehr.....	25
Tabelle 4: Faserkopplung bei MCFs nach [98].....	32
Tabelle 5: Vergleich DoFs für HD QKD.....	39
Tabelle 6: Übersicht Parameter HD QKD Systeme .....	40
Abbildung 1: Prozessschritte der CV QKD. ....	5
Abbildung 2: Typisches TF QKD Setup.....	11
Abbildung 3: Typische experimentelle SKR Werte und theoretische Grenzen für TF QKD im Vergleich zu BB84.....	14
Abbildung 4: Vergleich von passivem und aktivem Splitting .....	16
Abbildung 5: WDM 4-Nutzer-Star-Topologie .....	17
Abbildung 6: Wellenlängen-einsparende 5-Nutzer Sterntopologie.....	18
Abbildung 7: Down-/Up-Stream Quantum Access Network.....	18
Abbildung 8: 2xN TF QKD Realisierung.....	20
Abbildung 9: Schematische Darstellung eines passiven QKDNs basierend auf Verschränkung .....	21
Abbildung 10: Ringstruktur DPS mit Central Node und mehreren User Nodes.....	22
Abbildung 11: Qline Architektur.....	23
Abbildung 12: Ansätze zur Realisierung hybrider photonischer Chips. ....	28
Abbildung 13: 4D Time-Bin Codierung .....	37

## Literaturverzeichnis

- [1] F. Grosshans und P. Grangier, „Continuous Variable Quantum Cryptography Using Coherent States“, *Phys. Rev. Lett.*, Bd. 88, Nr. 5, S. 057902, Jan. 2002, doi: 10.1103/PhysRevLett.88.057902.
- [2] S. Pirandola u. a., „Advances in quantum cryptography“, *Adv. Opt. Photon., AOP*, Bd. 12, Nr. 4, S. 1012–1236, Dez. 2020, doi: 10.1364/AOP.361502.
- [3] Y. Zhang, Y. Bian, Z. Li, S. Yu, und H. Guo, „Continuous-variable quantum key distribution system: Past, present, and future“, *Applied Physics Reviews*, Bd. 11, Nr. 1, Art. Nr. 1, März 2024, doi: 10.1063/5.0179566.
- [4] Y. Tian u. a., „High-performance long-distance discrete-modulation continuous-variable quantum key distribution“, *Opt. Lett., OL*, Bd. 48, Nr. 11, S. 2953–2956, Juni 2023, doi: 10.1364/OL.492082.
- [5] H. H. Brunner, C.-H. F. Fung, und M. Peev, „CV-QKD Design for Network Integration“, in *2023 23rd International Conference on Transparent Optical Networks (ICTON)*, Juli 2023, S. 1–4. doi: 10.1109/ICTON59386.2023.10207256.
- [6] A. A. E. Hajomer, I. Derkach, N. Jain, H.-M. Chin, U. L. Andersen, und T. Gehring, „Long-distance continuous-variable quantum key distribution over 100 km fiber with local local oscillator“, 16. Mai 2023, *arXiv*: arXiv:2305.08156. doi: 10.48550/arXiv.2305.08156.
- [7] Y. Zhang u. a., „Long-Distance Continuous-Variable Quantum Key Distribution over 202.81 km of Fiber“, *Phys. Rev. Lett.*, Bd. 125, Nr. 1, S. 010502, Juni 2020, doi: 10.1103/PhysRevLett.125.010502.
- [8] Y. Bian u. a., „Continuous-variable quantum key distribution over 28.6 km fiber with an integrated silicon photonic receiver chip“, 15. Februar 2024, *arXiv*: arXiv:2402.10411. doi: 10.48550/arXiv.2402.10411.
- [9] G. Zhang u. a., „An integrated silicon photonic chip platform for continuous-variable quantum key distribution“, *Nat. Photonics*, Bd. 13, Nr. 12, S. 839–842, Dez. 2019, doi: 10.1038/s41566-019-0504-5.
- [10] Y. Zhang u. a., „Continuous-variable QKD over 50 km commercial fiber“, *Quantum Sci. Technol.*, Bd. 4, Nr. 3, S. 035006, Mai 2019, doi: 10.1088/2058-9565/ab19d1.
- [11] Y. Pi u. a., „Sub-Mbps key-rate continuous-variable quantum key distribution with local local oscillator over 100-km fiber“, *Opt. Lett., OL*, Bd. 48, Nr. 7, S. 1766–1769, Apr. 2023, doi: 10.1364/OL.485913.
- [12] H. Mani, T. Gehring, P. Grabenweger, B. Ömer, C. Pacher, und U. L. Andersen, „Multiedge-type low-density parity-check codes for continuous-variable quantum key distribution“, *Phys. Rev. A*, Bd. 103, Nr. 6, S. 062419, Juni 2021, doi: 10.1103/PhysRevA.103.062419.
- [13] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, und P. Grangier, „Multidimensional reconciliation for a continuous-variable quantum key distribution“, *Phys. Rev. A*, Bd. 77, Nr. 4, S. 042325, Apr. 2008, doi: 10.1103/PhysRevA.77.042325.
- [14] L. Chen, X.-M. Chen, und Y.-L. Yan, „Research on time-division multiplexing for error correction and privacy amplification in post-processing of quantum key distribution“, *Sci Rep*, Bd. 14, Nr. 1, S. 25326, Okt. 2024, doi: 10.1038/s41598-024-77047-9.
- [15] A. Leverrier, F. Grosshans, und P. Grangier, „Finite-size analysis of a continuous-variable quantum key distribution“, *Phys. Rev. A*, Bd. 81, Nr. 6, S. 062343, Juni 2010, doi: 10.1103/PhysRevA.81.062343.
- [16] H. H. Brunner u. a., „A low-complexity heterodyne CV-QKD architecture“, in *2017 19th International Conference on Transparent Optical Networks (ICTON)*, Juli 2017, S. 1–4. doi: 10.1109/ICTON.2017.8025030.

- [17] H. H. Brunner *u. a.*, „Demonstration of a switched CV-QKD network“, *EPJ Quantum Technol.*, Bd. 10, Nr. 1, Art. Nr. 1, Dez. 2023, doi: 10.1140/epjqt/s40507-023-00194-x.
- [18] „LuxQuanta“, LuxQuanta. Zugegriffen: 26. September 2024. [Online]. Verfügbar unter: <https://www.luxquanta.com/>
- [19] „KEEQuant“, KEEQuant. Zugegriffen: 26. September 2024. [Online]. Verfügbar unter: <https://www.keequant.com/>
- [20] M. Lucamarini, Z. L. Yuan, J. F. Dynes, und A. J. Shields, „Overcoming the rate–distance limit of quantum key distribution without quantum repeaters“, *Nature*, Bd. 557, Nr. 7705, S. 400–403, Mai 2018, doi: 10.1038/s41586-018-0066-6.
- [21] Y. Liu *u. a.*, „Experimental Twin-Field Quantum Key Distribution over 1000 km Fiber Distance“, *Phys. Rev. Lett.*, Bd. 130, Nr. 21, S. 210801, Mai 2023, doi: 10.1103/PhysRevLett.130.210801.
- [22] S. Wang *u. a.*, „Twin-field quantum key distribution over 830-km fibre“, *Nat. Photon.*, Bd. 16, Nr. 2, S. 154–161, Feb. 2022, doi: 10.1038/s41566-021-00928-2.
- [23] „(Part 4) The Future of Quantum Key Distribution Technology - Looking Towards the Coming Quantum Internet Age“, DiGiTAL T-SOUL. Zugegriffen: 17. Oktober 2024. [Online]. Verfügbar unter: <https://www.global.toshiba/ww/company/digitalsolution/articles/tsoul/tech/t0204.html>
- [24] M. Pittaluga, „Experimental repeater-like quantum communications over 600 km of optical fibre with dual-band phase stabilisation“, gehalten auf der qcrypt 2021, 2021. [Online]. Verfügbar unter: [https://2021.qcrypt.net/sessions/invited\\_pittaluga/](https://2021.qcrypt.net/sessions/invited_pittaluga/)
- [25] X.-B. Wang, Z.-W. Yu, und X.-L. Hu, „Twin-field quantum key distribution with large misalignment error“, *Phys. Rev. A*, Bd. 98, Nr. 6, S. 062323, Dez. 2018, doi: 10.1103/PhysRevA.98.062323.
- [26] J.-P. Chen *u. a.*, „Twin-Field Quantum Key Distribution with Local Frequency Reference“, *Phys. Rev. Lett.*, Bd. 132, Nr. 26, S. 260802, Juni 2024, doi: 10.1103/PhysRevLett.132.260802.
- [27] J.-P. Chen *u. a.*, „Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas“, *Nat. Photon.*, Bd. 15, Nr. 8, S. 570–575, Aug. 2021, doi: 10.1038/s41566-021-00828-5.
- [28] H. Du, T. K. Paraiso, M. Pittaluga, Y. S. Lo, J. A. Dolphin, und A. J. Shields, „Twin-field quantum key distribution with optical injection locking and phase encoding on-chip“, *Optica*, *OPTICA*, Bd. 11, Nr. 10, S. 1385–1390, Okt. 2024, doi: 10.1364/OPTICA.525743.
- [29] X. Zhong, W. Wang, R. Mandil, H.-K. Lo, und L. Qian, „Simple Multiuser Twin-Field Quantum Key Distribution Network“, *Phys. Rev. Appl.*, Bd. 17, Nr. 1, S. 014025, Jan. 2022, doi: 10.1103/PhysRevApplied.17.014025.
- [30] W. Li *u. a.*, „Twin-Field Quantum Key Distribution without Phase Locking“, *Phys. Rev. Lett.*, Bd. 130, Nr. 25, S. 250802, Juni 2023, doi: 10.1103/PhysRevLett.130.250802.
- [31] M. Pittaluga *u. a.*, „600-km repeater-like quantum communications with dual-band stabilization“, *Nature Photonics*, Bd. 15, S. 1–6, Juli 2021, doi: 10.1038/s41566-021-00811-0.
- [32] C. Clivati *u. a.*, „Coherent phase transfer for real-world twin-field quantum key distribution“, *Nat Commun*, Bd. 13, Nr. 1, S. 157, Jan. 2022, doi: 10.1038/s41467-021-27808-1.
- [33] M. Pittaluga *u. a.*, „Coherent Quantum Communications Across National Scale Telecommunication Infrastructure“, 21. Mai 2024, *arXiv*: arXiv:2405.11990. doi: 10.48550/arXiv.2405.11990.
- [34] A. Boaron *u. a.*, „Secure Quantum Key Distribution over 421 km of Optical Fiber“, *Phys. Rev. Lett.*, Bd. 121, Nr. 19, S. 190502, Nov. 2018, doi: 10.1103/PhysRevLett.121.190502.
- [35] C. H. Park *u. a.*, „2×N twin-field quantum key distribution network configuration based on polarization, wavelength, and time division multiplexing“, *npj Quantum Inf*, Bd. 8, Nr. 1, S. 1–12, Mai 2022, doi: 10.1038/s41534-022-00558-8.
- [36] X. Yu *u. a.*, „Secret-Key Provisioning With Collaborative Routing in Partially-Trusted-Relay-based Quantum-Key-Distribution-Secured Optical Networks“, *J. Lightwave Technol.*, Bd. 40, Nr. 12, S. 3530–3545, Juni 2022, doi: 10.1109/JLT.2022.3153992.
- [37] *Y.3800 : Overview on networks supporting quantum key distribution*. Zugegriffen: 22. Juli 2024. [Online]. Verfügbar unter: <https://www.itu.int/rec/T-REC-Y.3800/en>

- [38] J. Bogdanski, N. Rafiei, und M. Bourennane, „Multiuser quantum key distribution over telecom fiber networks“, *Optics Communications*, Bd. 282, Nr. 2, S. 258–262, Jan. 2009, doi: 10.1016/j.optcom.2008.10.030.
- [39] W. Chen u. a., „Field Experiment on a “Star Type” Metropolitan Quantum Key Distribution Network“, *IEEE Photonics Technology Letters*, Bd. 21, Nr. 9, S. 575–577, Mai 2009, doi: 10.1109/LPT.2009.2015058.
- [40] S. Wang u. a., „Field test of the wavelength-saving quantum key distribution network“, *Opt. Lett.*, Bd. 35, Nr. 14, S. 2454, Juli 2010, doi: 10.1364/OL.35.002454.
- [41] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, und A. J. Shields, „A quantum access network“, *Nature*, Bd. 501, Nr. 7465, S. 69–72, Sep. 2013, doi: 10.1038/nature12493.
- [42] R. Asif, „Quantum Secure Routing for Future Internet“, in *2020 International Conference on Information Networking (ICOIN)*, Barcelona, Spain: IEEE, Jan. 2020, S. 121–125. doi: 10.1109/ICOIN48656.2020.9016434.
- [43] O. Alia, R. S. Tessinari, E. Hugues-Salas, G. T. Kanellos, R. Nejabati, und D. Simeonidou, „Dynamic DV-QKD Networking in Trusted-Node-Free Software-Defined Optical Networks“, *J. Lightwave Technol.*, Bd. 40, Nr. 17, S. 5816–5824, Sep. 2022, doi: 10.1109/JLT.2022.3183962.
- [44] V. Martin u. a., „MadQCI: a heterogeneous and scalable SDN QKD network deployed in production facilities“, 3. Dezember 2023, *arXiv*: arXiv:2311.12791. doi: 10.48550/arXiv.2311.12791.
- [45] X. Zhong, W. Wang, R. Mandil, H.-K. Lo, und L. Qian, „Experiment on scalable multi-user twin-field quantum key distribution network“, 14. Juni 2021, *arXiv*: arXiv:2106.07768. doi: 10.48550/arXiv.2106.07768.
- [46] P. Xue, K. Wang, und X. Wang, „Efficient multiuser quantum cryptography network based on entanglement“, *Sci Rep*, Bd. 7, Nr. 1, S. 45928, Apr. 2017, doi: 10.1038/srep45928.
- [47] X. Hua, M. Hu, und B. Guo, „Multi-User Measurement-Device-Independent Quantum Key Distribution Based on GHZ Entangled State“, *Entropy*, Bd. 24, Nr. 6, Art. Nr. 6, Juni 2022, doi: 10.3390/e24060841.
- [48] S. K. Joshi u. a., „A trusted node-free eight-user metropolitan quantum communication network“, *Science Advances*, Bd. 6, Nr. 36, S. eaba0959, Sep. 2020, doi: 10.1126/sciadv.aba0959.
- [49] O. Alia, R. S. Tessinari, E. Hugues-Salas, G. T. Kanellos, R. Nejabati, und D. Simeonidou, „Wavelength Resources Management and Switching of Active Entanglement Distribution Circuits in Optical Networks“, in *2021 Optical Fiber Communications Conference and Exhibition (OFC)*, Juni 2021, S. 1–3. Zugegriffen: 4. November 2024. [Online]. Verfügbar unter: <https://ieeexplore.ieee.org/document/9489674/?arnumber=9489674>
- [50] X. Liu u. a., „40-user fully connected entanglement-based quantum key distribution network without trusted node“, *Photonix*, Bd. 3, Nr. 1, S. 2, Jan. 2022, doi: 10.1186/s43074-022-00048-2.
- [51] E. Fitzke u. a., „An Entanglement-Based QKD System for Scalable Robust Multi-User Networks“, in *2022 Conference on Lasers and Electro-Optics (CLEO)*, Mai 2022, S. 1–2. Zugegriffen: 6. November 2024. [Online]. Verfügbar unter: <https://ieeexplore.ieee.org/abstract/document/9890126>
- [52] E. Fitzke u. a., „A scalable network for simultaneous pairwise quantum key distribution via entanglement-based time-bin coding“, *PRX Quantum*, Bd. 3, Nr. 2, S. 020341, Mai 2022, doi: 10.1103/PRXQuantum.3.020341.
- [53] C. Autebert u. a., „Multi-user quantum key distribution with entangled photons from an AlGaAs chip“, *Quantum Sci. Technol.*, Bd. 1, Nr. 1, S. 01LT02, Dez. 2016, doi: 10.1088/2058-9565/1/1/01LT02.
- [54] Y. Bian, Y.-C. Zhang, C. Zhou, S. Yu, Z. Li, und H. Guo, „High-Rate Point-to-Multipoint Quantum Key Distribution using Coherent States“, 5. Februar 2023, *arXiv*: arXiv:2302.02391. doi: 10.48550/arXiv.2302.02391.

- [55] K. Inoue und T. Honjo, „Multiuser Differential-Phase-Shift Quantum Key Distribution System on a Ring Network“, *IEEE Photonics Technology Letters*, Bd. 36, Nr. 16, S. 989–992, Aug. 2024, doi: 10.1109/LPT.2024.3424432.
- [56] M. Doosti, L. Hanouz, A. Marin, E. Kashefi, und M. Kaplan, „Establishing shared secret keys on quantum line networks: protocol and security“, 4. April 2023, *arXiv*: arXiv:2304.01881. doi: 10.48550/arXiv.2304.01881.
- [57] M. Sena u. a., „Experimental validation of DV-QKD-based Qline architecture for metropolitan network on Berlin OpenQKD testbed“, in *49th European Conference on Optical Communications (ECOC 2023)*, Okt. 2023, S. 835–838. doi: 10.1049/icp.2023.2351.
- [58] „Q-bird-Flyer-technical-A5-v6-web.pdf“. Zugegriffen: 6. November 2024. [Online]. Verfügbar unter: <https://q-bird.com/wp-content/uploads/2024/10/Q-bird-Flyer-technical-A5-v6-web.pdf>
- [59] „PRODUCTS OVERVIEW“, Quantum Optics Jena. Zugegriffen: 6. November 2024. [Online]. Verfügbar unter: <https://qo-jena.com/products-overview/>
- [60] ITU-T, „Technical Report FG QIT4N D2.4 - Quantum key distribution network transport technologies“. 24. November 2021. Zugegriffen: 29. August 2024. [Online]. Verfügbar unter: <https://www.itu.int/en/ITU-T/focusgroups/qit4n/Documents/D2.4.pdf>
- [61] T. Dou u. a., „Coexistence of 11 Tbps (110×100 Gbps) classical optical communication and quantum key distribution based on single-mode fiber“, *Opt. Express, OE*, Bd. 32, Nr. 16, S. 28356–28369, Juli 2024, doi: 10.1364/OE.531364.
- [62] T. A. Eriksson u. a., „Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 Tbit/s data channels“, *Commun Phys*, Bd. 2, Nr. 1, S. 1–8, Jan. 2019, doi: 10.1038/s42005-018-0105-5.
- [63] M. Iqbal u. a., „SDN-Enabled Continuous-Variable QKD in Coexistence with 8×200 Gb/s 16-QAM Classical Channels“, in *2024 International Conference on Optical Network Design and Modeling (ONDM)*, Mai 2024, S. 1–3. doi: 10.23919/ONDM61578.2024.10582669.
- [64] P. Gavignet u. a., „Co-propagation of 6 Tb/s (60\*100Gb/s) DWDM & QKD channels with ~17 dBm aggregated WDM power over 50 km standard single mode fiber“, 23. Mai 2023, *arXiv*: arXiv:2305.13742. doi: 10.48550/arXiv.2305.13742.
- [65] J. Wang, B. J. Rollick, Z. Jia, und B. A. Huberman, „Time-Interleaved C-Band Co-Propagation of Quantum and Classical Channels“, *Journal of Lightwave Technology*, Bd. 42, Nr. 11, S. 4086–4095, Juni 2024, doi: 10.1109/JLT.2024.3381105.
- [66] S. Aleksic, F. Hipp, D. Winkler, A. Poppe, B. Schrenk, und G. Franzl, „Perspectives and limitations of QKD integration in metropolitan area networks“, *Opt. Express, OE*, Bd. 23, Nr. 8, S. 10359–10373, Apr. 2015, doi: 10.1364/OE.23.010359.
- [67] „Toshiba - Products“, Toshiba - Products. Zugegriffen: 29. August 2024. [Online]. Verfügbar unter: <https://www.global.toshiba/ww/products-solutions/security-ict/qkd/products.html>
- [68] „ID Quantique - Products“, ID Quantique - Products. Zugegriffen: 29. August 2024. [Online]. Verfügbar unter: <https://www.idquantique.com/quantum-safe-security/products/>
- [69] R. Wang u. a., „Field trial of a dynamically switched quantum network supporting co-existence of entanglement, prepare-and-measure QKD and classical channels“, in *49th European Conference on Optical Communications (ECOC 2023)*, Okt. 2023, S. 1682–1685. doi: 10.1049/icp.2023.2666.
- [70] L. Labonté u. a., „Integrated Photonics for Quantum Communications and Metrology“, *PRX Quantum*, Bd. 5, Nr. 1, S. 010101, Feb. 2024, doi: 10.1103/PRXQuantum.5.010101.
- [71] S. Saravi, T. Pertsch, und F. Setzpfandt, „Lithium Niobate on Insulator: An Emerging Platform for Integrated Quantum Photonics“, *Advanced Optical Materials*, Bd. 9, Nr. 22, S. 2100789, 2021, doi: 10.1002/adom.202100789.
- [72] A. Leinse, R. G. Heideman, E. J. Klein, R. Dekker, C. G. H. Roeloffzen, und D. A. I. Marpaung, „TriPlex™ platform technology for photonic integration: Applications from UV through NIR to IR“, in *2011 ICO International Conference on Information Photonics*, Mai 2011, S. 1–2. doi: 10.1109/ICO-IP.2011.5953782.



- [73] P. Sibson *u. a.*, „Chip-based Quantum Key Distribution“, 2. September 2015, *arXiv*: arXiv:1509.00768. Zugegriffen: 25. September 2024. [Online]. Verfügbar unter: <http://arxiv.org/abs/1509.00768>
- [74] P. Kaur, A. Boes, G. Ren, T. G. Nguyen, G. Roelkens, und A. Mitchell, „Hybrid and heterogeneous photonic integration“, *APL Photonics*, Bd. 6, Nr. 6, S. 061102, Juni 2021, doi: 10.1063/5.0052700.
- [75] J. A. Dolphin, T. K. Paraíso, H. Du, R. I. Woodward, D. G. Marangon, und A. J. Shields, „A hybrid integrated quantum key distribution transceiver chip“, *npj Quantum Inf*, Bd. 9, Nr. 1, S. 1–8, Sep. 2023, doi: 10.1038/s41534-023-00751-3.
- [76] L. Seidel *u. a.*, „Continuous-wave electrically pumped multi-quantum-well laser based on group-IV semiconductors“, *Nat Commun*, Bd. 15, Nr. 1, S. 10502, Dez. 2024, doi: 10.1038/s41467-024-54873-z.
- [77] T. K. Paraíso *u. a.*, „On-chip quantum secure communications“, in *Quantum Sensing and Nano Electronics and Photonics XIX*, SPIE, März 2023, S. 59–68. doi: 10.1117/12.2650036.
- [78] F. Beutel, H. Gehring, M. A. Wolff, C. Schuck, und W. Pernice, „Detector-integrated on-chip QKD receiver for GHz clock rates“, *npj Quantum Inf*, Bd. 7, Nr. 1, S. 1–8, Feb. 2021, doi: 10.1038/s41534-021-00373-7.
- [79] G. Zhang *u. a.*, „An integrated silicon photonic chip platform for continuous-variable quantum key distribution“, *Nat. Photonics*, Bd. 13, Nr. 12, S. 839–842, Dez. 2019, doi: 10.1038/s41566-019-0504-5.
- [80] R. Sax *u. a.*, „High-speed integrated QKD system“, *Photon. Res., PRJ*, Bd. 11, Nr. 6, S. 1007–1014, Juni 2023, doi: 10.1364/PRJ.481475.
- [81] K. Wei *u. a.*, „Resource-efficient quantum key distribution with integrated silicon photonics“, *Photon. Res., PRJ*, Bd. 11, Nr. 8, S. 1364–1372, Aug. 2023, doi: 10.1364/PRJ.482942.
- [82] P. Sibson, J. E. Kennard, S. Stanisic, C. Erven, J. L. O’Brien, und M. G. Thompson, „Integrated silicon photonics for high-speed quantum key distribution“, *Optica, OPTICA*, Bd. 4, Nr. 2, S. 172–177, Feb. 2017, doi: 10.1364/OPTICA.4.000172.
- [83] C. Ma *u. a.*, „Silicon photonic transmitter for polarization-encoded quantum key distribution“, *Optica, OPTICA*, Bd. 3, Nr. 11, S. 1274–1278, Nov. 2016, doi: 10.1364/OPTICA.3.001274.
- [84] Y. Bian *u. a.*, „Continuous-variable quantum key distribution over 28.6 km fiber with an integrated silicon photonic receiver chip“, *Applied Physics Letters*, Bd. 124, Nr. 17, S. 174001, Apr. 2024, doi: 10.1063/5.0203130.
- [85] Y.-H. Li *u. a.*, „On-Chip Multiplexed Multiple Entanglement Sources in a Single Silicon Nanowire“, *Phys. Rev. Applied*, Bd. 7, Nr. 6, S. 064005, Juni 2017, doi: 10.1103/PhysRevApplied.7.064005.
- [86] J. Wang *u. a.*, „Multidimensional quantum entanglement with large-scale integrated optics“, *Science*, Bd. 360, Nr. 6386, S. 285–291, Apr. 2018, doi: 10.1126/science.aar7053.
- [87] Q. Liu *u. a.*, „Advances in Chip-Based Quantum Key Distribution“, *Entropy*, Bd. 24, Nr. 10, Art. Nr. 10, Okt. 2022, doi: 10.3390/e24101334.
- [88] F. Jöhlinger *u. a.*, „Physical Security of Chip-Based Quantum Key Distribution Devices“, 29. August 2024, *arXiv*: arXiv:2408.16835. Zugegriffen: 26. September 2024. [Online]. Verfügbar unter: <http://arxiv.org/abs/2408.16835>
- [89] P. Sibson *u. a.*, „Field Trial of Quantum-Secured IPsec Tunnels with Chip-based QKD“, in *2024 Optical Fiber Communications Conference and Exhibition (OFC)*, März 2024, S. 1–4. Zugegriffen: 9. August 2024. [Online]. Verfügbar unter: <https://ieeexplore.ieee.org/document/10526644/?arnumber=10526644>
- [90] B. Zhu, „SDM Fibers for Data Center Applications“, 2019, [Online]. Verfügbar unter: <https://www.ofsoptics.com/wp-content/uploads/SDM-Fibers-for-Data-Center-Applications-paper-2019.pdf>
- [91] K. Saitoh und S. Matsuo, „Multicore fibers for large capacity transmission“, *Nanophotonics*, Bd. 2, Nr. 5–6, S. 441–454, Dez. 2013, doi: 10.1515/nanoph-2013-0037.

- [92] „ITU-T Technical Report GSTR-SDM (09/2022) Optical fibre, cable, and components for space division multiplexing transmission“, [Online]. Verfügbar unter: [https://www.itu.int/dms\\_pub/itu-t/opb/tut/T-TUT-HOME-2022-1-PDF-E.pdf](https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-HOME-2022-1-PDF-E.pdf)
- [93] D. S. Vaidya, „Perspectives on Multicore Fiber (MCF) Platforms vs. Incumbent Technology“.
- [94] R. Mercy Kingsta und R. Shantha Selvakumari, „A review on coupled and uncoupled multicore fibers for future ultra-high capacity optical communication“, *Optik*, Bd. 199, S. 163341, Dez. 2019, doi: 10.1016/j.ijleo.2019.163341.
- [95] S. Ö. Arik und J. M. Kahn, „Coupled-Core Multi-Core Fibers for Spatial Multiplexing“, *IEEE Photonics Technology Letters*, Bd. 25, Nr. 21, S. 2054–2057, Nov. 2013, doi: 10.1109/LPT.2013.2280897.
- [96] T. Hayashi, T. Taru, O. Shimakawa, T. Sasaki, und E. Sasaoka, „Design and fabrication of ultra-low crosstalk and low-loss multi-core fiber“, *Opt. Express, OE*, Bd. 19, Nr. 17, S. 16576–16592, Aug. 2011, doi: 10.1364/OE.19.016576.
- [97] A. M. Ortiz, R. L. Sáez, A. M. Ortiz, und R. L. Sáez, „Multi-Core Optical Fibers: Theory, Applications and Opportunities“, in *Selected Topics on Optical Fiber Technologies and Applications*, IntechOpen, 2017. doi: 10.5772/intechopen.72458.
- [98] T. Hayashi u. a., „Randomly-Coupled Multi-Core Fiber Technology“, *Proceedings of the IEEE*, Bd. 110, Nr. 11, S. 1786–1803, Nov. 2022, doi: 10.1109/JPROC.2022.3182049.
- [99] L. Sun u. a., „Theoretical investigations of weakly- and strongly-coupled multi-core fibers for the applications of optical submarine communications under power and fiber count limits“, *Opt. Express*, Bd. 31, Nr. 3, S. 4615, Jan. 2023, doi: 10.1364/OE.480344.
- [100] J. Sakaguchi u. a., „Large Spatial Channel (36-Core  $\times$  3 mode) Heterogeneous Few-Mode Multicore Fiber“, *Journal of Lightwave Technology*, Bd. 34, Nr. 1, S. 93–103, Jan. 2016, doi: 10.1109/JLT.2015.2481086.
- [101] B.-X. Wang u. a., „Long-distance transmission of quantum key distribution coexisting with classical optical communication over a weakly-coupled few-mode fiber“, *Opt. Express*, Bd. 28, Nr. 9, S. 12558, Apr. 2020, doi: 10.1364/OE.388857.
- [102] X. Yu, S. Li, Y. Zhao, Y. Cao, A. Nag, und J. Zhang, „Routing, Core and Wavelength Allocation in Multi-Core-Fiber-Based Quantum-Key-Distribution-Enabled Optical Networks“, *IEEE Access*, Bd. 9, S. 99842–99852, 2021, doi: 10.1109/ACCESS.2021.3096879.
- [103] J. F. Dynes u. a., „Quantum key distribution over multicore fiber“, *Opt. Express*, Bd. 24, Nr. 8, S. 8081, Apr. 2016, doi: 10.1364/OE.24.008081.
- [104] T. Hayashi u. a., „Field-Deployed Multi-Core Fiber Testbed“, in *2019 24th OptoElectronics and Communications Conference (OECC) and 2019 International Conference on Photonics in Switching and Computing (PSC)*, Juli 2019, S. 1–3. doi: 10.23919/PS.2019.8818058.
- [105] M. Zahidy u. a., „Practical high-dimensional quantum key distribution protocol over deployed multicore fiber“, *Nat Commun*, Bd. 15, Nr. 1, S. 1651, Feb. 2024, doi: 10.1038/s41467-024-45876-x.
- [106] M. Zahidy u. a., „4-Dimensional Quantum Key Distribution Protocol over 52-km Deployed Multicore Fibre“, in *2022 European Conference on Optical Communication (ECOC)*, Sep. 2022, S. 1–4. Zugegriffen: 12. August 2024. [Online]. Verfügbar unter: <https://ieeexplore.ieee.org/document/9979604>
- [107] X. Wang u. a., „Field Trial of  $7 \times 89\lambda \times 256$  Gb/s C-Band Classical / CVQKD Co-Existence Transmission over 7-Core Fiber“, in *2023 Asia Communications and Photonics Conference/2023 International Photonics and Optoelectronics Meetings (ACP/POEM)*, Nov. 2023, S. 1–4. doi: 10.1109/ACP/POEM59049.2023.10369872.
- [108] E. Hugues-Salas u. a., „Coexistence of 11.2Tb/s Carrier-Grade Classical Channels and a DV-QKD Channel over a 7-Core Multicore Fibre“, 2. Juli 2019, *arXiv*: arXiv:1907.01459. doi: 10.48550/arXiv.1907.01459.
- [109] E. Hugues-Salas u. a., „11.2 Tb/s Classical Channel Coexistence With DV-QKD Over a 7-Core Multicore Fiber“, *Journal of Lightwave Technology*, Bd. 38, Nr. 18, S. 5064–5070, Sep. 2020, doi: 10.1109/JLT.2020.2998053.

- [110] R. Lin *u. a.*, „Telecommunication Compatibility Evaluation for Co-existing Quantum Key Distribution in Homogenous Multicore Fiber“, *IEEE Access*, Bd. 8, S. 78836–78846, 2020, doi: 10.1109/ACCESS.2020.2990186.
- [111] D. Bacco *u. a.*, „Boosting the secret key rate in a shared quantum and classical fibre communication system“, *Commun Phys*, Bd. 2, Nr. 1, S. 140, Nov. 2019, doi: 10.1038/s42005-019-0238-1.
- [112] J.-Q. Geng *u. a.*, „Integration in the C-band between quantum key distribution and the classical channel of 25 dBm launch power over multicore fiber media“, *Opt. Lett., OL*, Bd. 47, Nr. 12, S. 3111–3114, Juni 2022, doi: 10.1364/OL.463545.
- [113] W. Kong *u. a.*, „Enhanced Coexistence of Quantum Key Distribution and Classical Communication over Hollow-Core and Multi-Core Fibers“, *Entropy*, Bd. 26, Nr. 7, Art. Nr. 7, Juli 2024, doi: 10.3390/e26070601.
- [114] K. Zhou, L. Zhu, G. Sun, und Y. He, „FBG-based 3D shape sensor based on spun multi-core fibre for continuum surgical robots“, *Appl. Phys. B*, Bd. 129, Nr. 9, S. 140, Aug. 2023, doi: 10.1007/s00340-023-08082-z.
- [115] D. Cozzolino, B. Da Lio, D. Bacco, und L. K. Oxenløwe, „High-Dimensional Quantum Communication: Benefits, Progress, and Future Challenges“, *Advanced Quantum Technologies*, Bd. 2, Nr. 12, Art. Nr. 12, 2019, doi: 10.1002/qute.201900038.
- [116] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, und D. J. Gauthier, „Provably-Secure and High-Rate Quantum Key Distribution with Time-Bin Qudits“, *Sci. Adv.*, Bd. 3, Nr. 11, S. e1701491, Nov. 2017, doi: 10.1126/sciadv.1701491.
- [117] I. Vagniluca *u. a.*, „Efficient Time-Bin Encoding for Practical High-Dimensional Quantum Key Distribution“, *Phys. Rev. Appl.*, Bd. 14, Nr. 1, S. 014051, Juli 2020, doi: 10.1103/PhysRevApplied.14.014051.
- [118] G. A. H. Natarajan, und V. Raghunathan, „Fiber-based higher dimensional quantum key distribution implementation using time-bin qudits“, in *Quantum Computing, Communication, and Simulation IV*, SPIE, März 2024, S. 111–118. doi: 10.1117/12.3002155.
- [119] G. A. H. Natarajan, V. Raghunathan, und A. Polley, „Field Implementation of Higher Dimensional Time-bin Encoded Quantum Key Distribution Within IISc Campus“, in *2024 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, Juli 2024, S. 1–5. doi: 10.1109/CONECCT62155.2024.10677090.
- [120] J. Liu *u. a.*, „High-dimensional quantum key distribution using energy-time entanglement over 242 km partially deployed fiber“, *Quantum Sci. Technol.*, Bd. 9, Nr. 1, S. 015003, Okt. 2023, doi: 10.1088/2058-9565/acfe37.
- [121] B. Da Lio *u. a.*, „Path-encoded high-dimensional quantum communication over a 2-km multicore fiber“, *npj Quantum Inf*, Bd. 7, Nr. 1, S. 1–6, Apr. 2021, doi: 10.1038/s41534-021-00398-y.
- [122] M. Mafu *u. a.*, „Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases“, *Phys. Rev. A*, Bd. 88, Nr. 3, Art. Nr. 3, Sep. 2013, doi: 10.1103/PhysRevA.88.032305.
- [123] D. Cozzolino *u. a.*, „Orbital angular momentum states enabling fiber-based high-dimensional quantum communication“, arXiv.org. Zugegriffen: 11. September 2024. [Online]. Verfügbar unter: <https://arxiv.org/abs/1803.10138v2>
- [124] D. Cozzolino *u. a.*, „Air-core fiber distribution of hybrid vector vortex-polarization entangled states“, *Adv. Photon.*, Bd. 1, Nr. 04, S. 1, Aug. 2019, doi: 10.1117/1.AP.1.4.046005.
- [125] E. Otte, A. D. White, N. A. Günsken, J. Vučković, und M. L. Brongersma, „Tunable vector beam decoder by inverse design for high-dimensional quantum key distribution with 3D polarized spatial modes“, 25. April 2023, arXiv: arXiv:2304.12296. Zugegriffen: 18. September 2024. [Online]. Verfügbar unter: <http://arxiv.org/abs/2304.12296>
- [126] M. C. Ponce, A. L. M. Muniz, M. Huber, und F. Steinlechner, „High-Dimensional Entanglement for Quantum Communication in the Frequency Domain“, *Laser & Photonics Reviews*, Bd. 17, Nr. 9, S. 2201010, Sep. 2023, doi: 10.1002/lpor.202201010.

- [127] M. Kues *u. a.*, „On-chip generation of high-dimensional entangled quantum states and their coherent control“, *Nature*, Bd. 546, Nr. 7660, S. 622–626, Juni 2017, doi: 10.1038/nature22986.
- [128] D.-X. Chen, J. Jia, P. Zhang, und C.-P. Yang, „Optimized architectures for universal quantum state transformations using photonic path and polarization“, *Quantum Sci. Technol.*, Bd. 8, Nr. 1, S. 015011, Nov. 2022, doi: 10.1088/2058-9565/aca11b.
- [129] F. Steinlechner *u. a.*, „Distribution of high-dimensional entanglement via an intra-city free-space link“, *Nat Commun*, Bd. 8, Nr. 1, S. 15971, Juli 2017, doi: 10.1038/ncomms15971.
- [130] J. Nunn, L. J. Wright, C. Söller, L. Zhang, I. A. Walmsley, und B. J. Smith, „Large-alphabet time-frequency entangled quantum key distribution by means of time-to-frequency conversion“, *Opt. Express, OE*, Bd. 21, Nr. 13, S. 15959–15973, Juli 2013, doi: 10.1364/OE.21.015959.
- [131] F.-X. Wang *u. a.*, „Hybrid High-Dimensional Quantum Key Distribution for a Composable Quantum Network“, *Phys. Rev. Applied*, Bd. 19, Nr. 5, S. 054060, Mai 2023, doi: 10.1103/PhysRevApplied.19.054060.